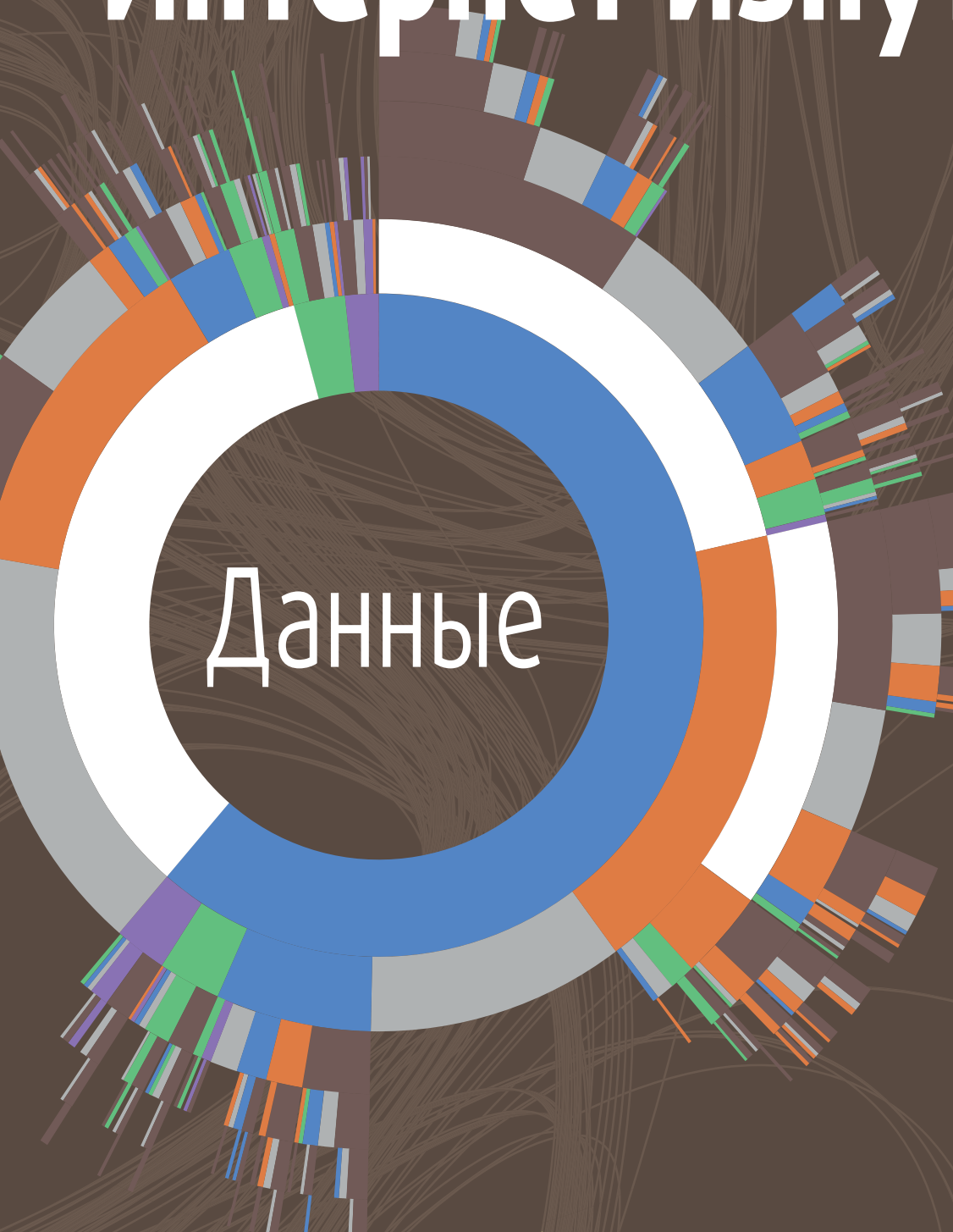
№6
май 2017

MSK IX

Интернет изнутри



Данные

Утечки данных. Проблематика

Почему организации не делают все возможное для профилактики утечек и снижения ущерба?

Содержание:

Журнал «Интернет изнутри»
По всем вопросам пишите на info@internetinside.ru

Порядковый номер выпуска и дата его выхода в свет:
Выпуск №6, дата выхода: май 2017 г.

Свидетельство о регистрации СМИ в Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций. Регистрационный номер:
Эл № ФС77-63308

Публикуется при поддержке АНО «ЦВКС «МСК-IX»

Главный редактор:
Андрей Робачевский

Зам. главного редактора:
Новикова Татьяна

Редакционная коллегия:
Воронина Елена
Платонов Алексей

Дизайн:
Чернега Наталья

Корректор:
Рябова Наталья

главный редактор,
Андрей Робачевский

Новая нефть

Дорогой читатель!

Неслучайно данные, и особенно – персональные данные называют новой нефтью. Они являются основой успешных бизнес-моделей многих интернет-услуг, наиболее распространенной из которых является модель посредничества между потребителями - пользователями онлайн-платформ и рекламодателями. Эта модель остается весьма прибыльной, если посмотреть на растущие доходы ведущих игроков в этой области. Например, доходы Google от онлайн-рекламы за прошлый год достигли 79,4 миллиарда долларов США. Это больше, чем ВНП многих стран.

Но данные также являются хрупким, или лучше сказать - текучим активом. Мы читаем о краже сотни миллионов учетных записей пользователей, десятков миллионов кредитных карт, гигабайтов электронной переписки, терабайтов разнообразной конфиденциальной информации... Этому списку нет конца. Можно предположить, что о многих утечках просто не известно - ведь данные не крадут - их копируют.

Этот номер посвящен данным, в первую очередь защите данных от утечек - об этом вы сможете прочитать в избранных главах отчета "Утечки данных: Проблематика". Также мы познакомим вас с законодательными аспектами защиты персональных данных в разных странах мира.

И конечно, мы включили некоторые технологические аспекты, связанные с данными: как наиболее эффективно доставить данные пользователю или какую роль играют данные в построении интеллектуальных сетей нового поколения.

От 120-байтных перфокарт до бытовых 10-терабайтных дисков, от BBS (электронной доски объявлений) до мощных сетей доставки контента и облачных услуг - этот удивительный прогресс только ускоряется. Как отметил в 2010 году в то время генеральный директор Google Эрик Шмидт, "с момента зарождения нашей цивилизации до 2003 года включительно человечество произвело 5 экзабайт данных. Сегодня это же количество информации производится каждые два дня". Уверен, что его цитата уже устарела.

Перед вами шестой выпуск. Надеемся, что он оправдает ваши ожидания. Расскажите нам, что вам понравилось, а что – нет, о чем бы вы хотели прочитать в следующих номерах. Ждем ваших отзывов и предложений по адресу info@internetinside.ru.

Утечки данных. Проблематика

Избранные главы «Отчета о глобальном Интернете 2016», Global Internet Report 2016

Проблем, связанных с утечками данных, включая их причины, последствия и решения по предотвращению, имеется огромное количество. Источниками утечек могут быть как внешние атаки (инициированные хакерами-активистами, хакерами на государственной службе или лицами, ищущими финансовой выгоды), так и атаки инсайдеров (со своим комплексом мотиваций) или даже случайные потери. В этой статье мы сосредоточимся на ряде постоянно возникающих проблем и выработаем рекомендации по их решению.

Во-первых, масштаб утечек данных может быть обширным и многогранным. При взломе сети супермаркетов Target (http://krebsonsecurity.com/2014/05/the-target-breach-by-the-numbers/) значительные финансовые убытки понесли сама компания Target, банки (вынужденные перевыпустить скомпрометированные кредитные карты) и клиенты, которым потребовалось разбираться с мошенничеством в результате утечки. При взломе сайта знакомств Ashley Madison (https://securityintelligence.com/two-important-lessons-from-the-ashley-madison-breach/) убытки далеко не исчерпывались финансовой стороной, так как на всеобщее обозрение оказалась выставлена личная жизнь пользователей. При взломе Управления кадровой службы США (https://arstechnica.com/security/2015/06/report-hack-of-government-employee-records-discovered-by-product-demo/32/) дело зашло еще дальше огласки обстоятельств личной жизни сотрудников и других лиц: оказалось, что возможно установить личность ряда сотрудников по украденной биометрической информации, и последствия этого трудно предугадать.

Перед лицом потерь такого масштаба, как финансовых, так и нет, трудно себе представить, что многие из этих утечек можно было предотвратить, так как взломщики использовали известные уязвимости. Для некоторых из них имелись патчи, но их не установили. В ряде случаев злоумышленники использовали человеческий фактор, применяя методы социального инжиниринга, которые опять же давно известны и против которых имеется защита.

Разумеется, не все утечки возникают в результате хакерских атак и не все атаки можно предотвратить. Некоторые атаки используют так называемые уязвимости нулевого дня (zero-day exploits), о которых не было известно до момента взлома. Другие утечки становятся результатом случайного разглашения данных, например, в случае утери устройства с конфиденциальной информацией. Разумеется, такие утечки предотвратить невозможно, но учитывая, насколько часто такое случается, их как минимум можно ожидать, а следовательно, и минимизировать ущерб от них.

Главный вопрос, который здесь возникает, – «почему?» Почему, учитывая цену утечки, компании не сделали больше для того, чтобы предотвратить то, что можно, и снизить воздействие того, что предотвратить нельзя? И здесь на первый план выходит экономика доверия.

В этой статье опишем действия, которые можно было предпринять для профилактики атак и минимизации их последствий, а затем дадим ответ, с точки зрения экономики, на вопрос, почему же эти меры не принимаются повсеместно.

Бреши в системе безопасности

Многие атаки можно предотвратить

Потрясает тот факт, что многие атаки, если не большинство из них, можно было предотвратить за счет современных систем безопасности и обучения сотрудников безопасной работе с данными и противодействию социальному инжинирингу. В одном из недавних исследований известных утечек утверждается, что 93% из них можно было избежать (см. https://otalliance.org/resources/data-breach-protection).

Известные уязвимости

По данным Verizon, 70% атак извне используют известные уязвимости, некоторые из которых существуют еще с 1999 года. Verizon ежегодно публикует отчет о расследованиях утечек данных (Data Breach Investigations Report). В отчете за 2015 год имеется раздел об использовании известных уязвимостей, который мы здесь и цитируем (см. http://www.verizonenterprise.com/verizon-insights-lab/dbir/, с. 15-17). Для анализа известных уязвимостей Verizon использует базу данных Common Vulnerabilities and Exposures (CVE), определяемую как «список уязвимостей и пробелов в информационной безопасности, предназначенный для присвоения общих имен известным проблемам кибербезопасности. Целью CVE является облегчение совместного использования данных в разных средствах борьбы с уязвимостями (инструменты, репозитории, сервисы) благодаря общему именованию». CVE спонсируется US-CERT в составе министерства внутренней безопасности США и управляется MITRE (http://cve.mitre.org/). В отчете Verizon перечислено десять известных уязвимостей,

на чью долю пришлось почти 97% атак в 2014 году и 85% в 2015-м (http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/). Эти уязвимости абсолютно необходимо закрыть патчами, но даже после этого остается длинный список известных «дырок».

Та же проблема, только под другим углом, освещается еще в одном отчете. Symantec сообщает, что 78% просканированных веб-сайтов содержали известные уязвимости. Более того, 15% из них были критическими, т.е. открывали дорогу вредоносному коду, который мог привести к утечкам данных и компрометации посетителей сайтов (https://www.symantec.com/security-center/threat-report).

Ярким примером проблем с безопасностью является то, что многие интернет-атаки проводятся через плагины сторонних разработчиков. Это в том числе и браузерные плагины, такие как Adobe Flash Player, на долю которого за прошедшие годы пришлось множество атак, включая значительную часть уязвимостей нулевого дня.

Проблемы с плагинами относятся не только к браузерам, но и к сайтам. 25% всех веб-сайтов в мире основаны на WordPress, где свой плагин может написать каждый. Плагины расширяют функционал веб-сайтов, например, облегчают ввод контактных данных, но в то же время могут быть уязвимы для атак, таких как SQL-инъекции.

Одни и те же функции придают плагинам и ценность, и уязвимость. Плагины позволяют независимым разработчикам добавлять новый функционал к используемой программной платформе. Готовые решения, такие как Adobe Flash, облегчают предоставление контента пользователю, упрощая работу контент-провайдеров. Это способствует повышению доступности контента. Но в то же время увеличивается и количество мишеней для атак, поскольку пользовательская аудитория существенно больше, а плагины можно разрабатывать и устанавливать независимо от платформы, что сужает возможности проверки ПО и предотвращения атак.

Хотя и не все атаки на веб-сайты проводятся через плагины, этот пример хорошо иллюстрирует комплекс проблем, возникающих при открытии платформы для ПО сторонних разработчиков, безопасность которого не гарантирована.

Социальный инжиниринг

Социальный инжиниринг – это распространенный метод, с помощью которого хакеры получают доступ к закрытой системе. Он заключается в том, что сотрудника обманным путем вынуждают сообщить свой пароль или даже своими руками привнести инфекцию в систему. Одна из популярных практик называется «фишингом» (phishing). Пользователям рассылается официального вида письмо, которое либо содержит вредоносное вложение, либо предписывает залогиниться на подставном сайте. Более узконаправленной (и прибыльной) разновидностью фишинга является направленный фишинг (spearphishing). По имеющимся данным, фишинговые кампании очень эффективны, даже против организаций, работающих в сфере информационной безопасности. Именно этот метод был использован для атаки на Target, с заходом через поставщика холодильного оборудования. Согласно Verizon, в одном из тестов с рассылкой 150 тысяч электронных писем 50% пользователей уже в первый час после рассылки открыли письма и щелкнули по фишинговым ссылкам. Первый «щелчок» произошел всего через 82 секунды.

Но арсенал социального инжиниринга отнюдь не ограничивается фишингом. Проводились эксперименты с разбрасыванием «флэшек» (USB-накопителей) на корпоративных парковках и в других подобных местах. Почти половину из них нашли и вставили в устройства, причем первую – всего через 6 минут (См. https://nakedsecurity.sophos.com/2016/04/08/almost-half-of-dropped-usb-sticks-will-get-plugged-in/). В экспериментах «флэшка» просто сообщала, что система прочла ее, но таким способом можно было легко занести на компьютер вредоносный код.

Опасность социального инжиниринга усугубляется современными тенденциями организации работы. Все больше людей берут работу на дом, и все больше компаний разрешают сотрудникам использовать для работы личное оборудование (PC или мобильные устройства), которое может быть плохо защищено. Таким образом, IT-системы компаний становятся уязвимыми для атак, направленных на сотрудников. Не облегчает задачу и склонность людей иметь как можно меньше разных паролей. Если кто-либо использует один и тот же пароль в своей личной и профессиональной жизни, то фишинговые атаки ставят под угрозу безопасность систем его работодателя, в потенциале приводя к утечке данных.

Не все атаки можно предотвратить

Защититься от всех киберинцидентов невозможно. Некоторые из них используют ранее не известные либо неустранимые проблемы безопасности. Другие возникают в результате случайной потери или публикации данных. Но абсолютно во всех случаях можно смягчить последствия инцидента. Как отмечалось в отчете OTA 2016, «...мы обнаружили, что неуязвимых организаций не бывает. По мере того, как набираются большие объемы разнородных данных и все больше приходится полагаться на внешних поставщиков услуг, каждой компании следует быть готовой к неизбежной потере данных. Факты подчеркивают, что и стартапам, и глобальным корпорациям следует радикально изменить отношение и сделать безопасность и конфиденциальность данных обязанностью каждого сотрудника» (https://otalliance.org/resources/data-breach-protection).

Неизвестные уязвимости

Хотя от известных проблем безопасности можно защититься, ни одна из них не стала известной сразу же. Это так называемые уязвимости нулевого дня.

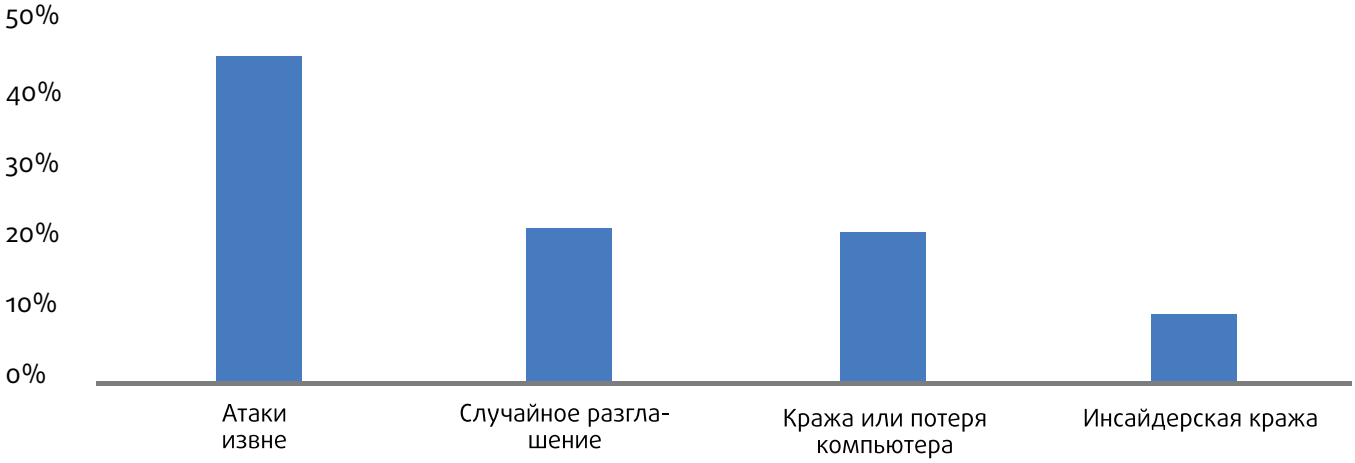
По данным Symantec, количество уязвимостей нулевого дня в последние годы выросло: в 2013 году их было 14, в 2014 – уже 24, а в 2015 – целых 54. Разумеется, они по определению известны еще не все: вполне возможно, что некоторые из них терпеливо ждут своего часа... или покупателя.

Существует целый черный рынок уязвимостей нулевого дня, где покупателями являются хакеры, спецслужбы и компании-разработчики программного обеспечения. Как только уязвимость использована, она не теряет опасности полностью, а по-прежнему может применяться против тех, кто еще не закрыл эту брешь.

Рыночные цены на уязвимости нулевого дня зависят от мишени для атаки, но могут дойти до весьма крупных цифр – например, 250 тысяч долларов за недавнюю уязвимость в Apple iOS. Есть и «белый рынок»: разработчики ПО могут предлагать деньги за обнаружение брешей в собственной продукции, но, как правило, тут цены не поднимаются выше 10 тысяч долларов.

И, наконец, некоторые из уязвимостей нулевого дня намеренно добавляются в ПО авторами. Например, подобные лазей-

Рис. 1. Основные причины утечек (% случаев утечки), Источник: Symantec Internet Security Threats Report, 2016.



ки в своей продукции создает компания Hacking Team, разрабатывающая шпионское ПО для спецслужб разных стран. Многие из этих лазеек были преданы гласности в результате атаки на саму Hacking Team и быстро вошли в состав эксплоит-китов, таких как Angler, став доступными широкому кругу хакеров.

Инсайдерские действия

Атаки извне, согласно большинству исследований, составляют основную массу атак, но сотрудники тоже вносят свою «лепту» в утечки данных: кто по злому умыслу, кто по невнимательности. Ниже приведена сводка инцидентов за 2015 год по данным Symantec.

Ошибки делают все: кто-то пишет программу с багами, кто-то теряет USB-ключ, кто-то принимает на работу не того, кого следовало, – и некоторые из таких ошибок приводят к утечкам данных. Как мы подробно рассмотрим в разделе рекомендаций, гораздо безопаснее проектировать технологию с учетом человеческого фактора, чем пытаться переделать людей. См. рис. 1.

Организации могут снизить ущерб от атаки

Профилактика очень важна для защиты от «широкополосных», таких как фишинг, и даже от более узконаправленных атак, таких как направленный фишинг. Однако она не должна быть единственным рубежом защиты, потому что при достаточном желании хакер рано или поздно добьется своего.

Принимая во внимание, что даже в лучшем случае утечка данных возможна, а в худшем случае – вполне вероятна, следует по крайней мере свести к минимуму потенциальный вред от нее. Полный список таких мер длинен и требует разработки крупномасштабной стратегии с применением различных технических средств, таких как средства раннего обнаружения, обучение персонала, правовая защита и коммуникационный план. Обзор спектра затронутых проблем приведен в отчете OTA 2016 по адресу https://otalliance.org/resources/data-breachprotection.

Приведем два простых способа снизить воздействие утечки.

- во-первых, хранить как можно меньше данных: нет данных – нет и утечки;
- во-вторых, использовать шифрование: похищенные данные не имеют ценности, если их невозможно прочесть.

Более подробно эти принципы описаны в разделе рекомендаций.

Все возрастающее число устройств и датчиков, собирающих данные, наша деятельность онлайн, генерирующая данные, и венчурные компании в поисках «следующего мегахита» дополняются падением цен на устройства хранения данных, создавая идеальный информационный шторм для Big Data.

Однако, как отметил эксперт по кибербезопасности Брюс Шнейер, такие данные могут стать «ядовитым активом» (https://www.schneier.com/blog/archives/2016/03/data_is_a_toxic.html). Ущерб от утечки данных может во много раз перевесить преимущества, которые эти данные принесли бы при использовании по назначению.

Разумеется, можно минимизировать число собираемых данных, но совсем обойтись без этого не всегда получится. Поэтому компаниям следует снизить потенциальный ущерб от потери любых сохраненных данных путем адекватного шифрования – данные, которые нельзя прочесть, нельзя и использовать.

Многие организации не имеют стандартных практик по снижению объема собираемых данных и шифрованию имеющихся. А ведь эти меры защиты настолько очевидны, что трудно понять, почему же их не принимают. Ответ на этот вопрос дает экономика.

Экономика утечек данных

Почему организации не делают все возможное для профилактики утечек и снижения ущерба?

Экономика утечек данных и их воздействия на доверие – эта тема является центральной в этой статье. Мы рассмотрим некоторые разновидности ущерба от утечек, который может быть весьма высоким, и некоторые из их причин.

Предотвратить можно не все утечки, но многие. Например, Target взломали через соединение с поставщиком холодильного оборудования. Один из сотрудников поставщика из-за неадекватной антивирус-

ной защиты стал жертвой фишинга. Далее вредоносный код заразил кассовые терминалы Target и начал собирать данные с них – скорее всего, из-за слабых или стандартных паролей в одной или нескольких системах. Обучали ли сотрудника рискам и опасностям фишинговых атак? Почему администратор счел достаточной домашнюю версию антивируса? Проверял ли вообще Target информационную безопасность подрядчика перед заключением контракта? Почему стандартные пароли никто не поменял?

Аналогичный вопрос: можно ли снизить ущерб от утечки постфактум? После взлома TalkTalk гендиректор компании сначала заявила, что не знает, были ли украденные данные клиентов зашифрованы. Потом признала, что зашифрованы они не были, но все равно утверждала, что компания выполнила все требования регулирующих органов. Как случилось, что генеральный директор крупного провайдера не знал, зашифрованы данные клиентов или нет, на момент третьего подряд инцидента IT-безопасности?

В истории с Ashley Madison некоторые из лиц, чья личная информация попала в открытый доступ, заплатили компании по 19 долларов за удаление своих данных: значит, это либо не было сделано вообще, либо было сделано неправильно. Брать деньги за удаление данных о клиентах – не самая распространенная практика, но это теоретически можно списать на специфический характер бизнеса Ashley Madison. Другой вопрос: как можно предлагать клиентам платную услугу по удалению данных и не удалять их как следует?

Вернемся к Target. Покрыл ли поставщик холодильного оборудования, через которого была проведена первая атака, хоть какие-то затраты? Впрочем, Target и сама покрыла далеко не все убытки от взлома. Банки потратили не менее 240 миллионов долларов на перевыпуск скомпрометированных кредитных карт, хотя часть этих денег они смогли отсудить.

Последствия утечек также вскрывают некоторые интересные обстоятельства. Клиенты Ashley Madison никак не могли знать, защищены ли их данные: возникает вопрос, могла бы другая служба знакомств получить конкурентное преимущество, просто заявив, что у них защита данных лучше? Почему же компании не делают большего для того, чтобы предотвратить или снизить риск утечки данных?

С точки зрения экономики, мы можем объяснить это при помощи двух концепций, сводящихся просто-напросто к затратам и преимуществам. Вкратце говоря, убытки от утечки не целиком ложатся на плечи пострадавшей организации, а преимущества от лучшей защиты данных оказываются недостаточно высоки.

Экстерналии

Крайне редко бывает, чтобы убытки понес только сборщик данных, которого взломали: убытки, понесенные другими сторонами, в экономике называются экстерналиями.

- Когда гендиректор Ashley Madison принимал решение о том, сколько денег потратить на защиту информации (в том числе о собственных внебрачных связях, ставших достоянием общественности в результате взлома), он вряд ли думал о полном масштабе последствий возможной утечки для других.

- Хотя компания Target и понесла значительные убытки в результате утечки, не ей пришлось оплачивать перевыпуск карт всех покупателей: это бремя легло на банки.

- Взлом AOL-аккаунта директора ЦРУ, в результате чего тот был вынужден бросить все дела и разбираться с последствиями публикации своих личных писем в Интернете, был осуществлен на основе информации, выуженной у сотрудника Verizon.

В тех странах, где сообщать об утечке необязательно, экстерналии еще драматичнее, а сама компания может вообще не понести репутационных потерь, что еще более снижает мотивацию вкладываться в кибербезопасность.

Кроме того, утечки данных ослабляют уровень доверия в будущем – как для тех, кто был затронут инцидентом, так и для тех, кто о нем только слышал. В результате люди начинают неохотнее выходить в Интернет, а выйдя, избегают услуг, требующих ввода личной информации, что в свою очередь ограничивает рост интернет-экономики. Удар по доверию – тоже одна из экстерналий, а с экономической точки зрения у организации нет ни причин, ни стимулов отвечать за ущерб, нанесенный всему Интернету в результате ее решений по профилактике утечек и ликвидации их последствий. Но общество пренебречь этим не может.

Асимметричная информация

Неравный уровень информированности о возможных рисках у разных сторон одной сделки (т.н. асимметричная информация) затрудняет принятие рациональных решений. В частности, организациям становится труднее получать выгоду от правильных действий по борьбе с утечками данных. Target ведь не может проверить антивирусы у всех подрядчиков; так и директор ЦРУ не может знать, насколько хорошо Verizon обучает сотрудников бороться с социальным инжинирингом. Но и это еще не предел. Ashley Madison никак не может доказательно продемонстрировать, что сделала все возможное для защиты данных нынешних клиентов, и что данные о тех, кто заплатил за удаление, действительно были удалены.

Асимметричная информация ведет к проблемам неблагоприятного отбора и морального риска, давно описанным в экономической науке.

К примеру, пусть некий интернет-магазин, боясь взлома, хочет принять меры к защите компании от утечки данных.

Предположим, что этот магазин решил вложить значительную сумму в защиту информации о пользователях от хакеров, чтобы получить конкурентное преимущество перед другими, хуже защищенными торговыми площадками. Как он убедит пользователей в своей надежности? Можно, конечно, заявить, что их еще ни разу не взломали, но разве это гарантия? Если продемонстрировать надежность никак нельзя, то нельзя и привлечь ею клиентов, а потому вступает в силу неблагоприятный отбор: преимущество на рынке получают те, кто на безопасность не тратился.

Если руководство магазина все-таки боится утечки данных, то вместо адекватных инвестиций в безопасность оно может купить страховку от киберугроз (тут опять вступает в силу неблагоприятный отбор: страхуются чаще те, кто подвержен наибольшему риску). Теперь уже активизируется моральный риск: страховка есть, значит можно еще меньше вкладывать в кибербезопасность, потому что цена утечки становится еще ниже (а сама утечка – еще более вероятной).

Разумеется, это утрированный пример, и наверняка существует множество компаний, которые полностью осознают цену утечки данных и мудро инвестируют в их

защиту. Тем не менее, из этого примера уже виден ряд значительных проблем, не решив которых, ситуацию с безопасностью не переломить. В частности, нет способа убедительно показать наличие мер безопасности и их действенность.

Экономический ликбез

Экстерналии и асимметрия информации – признаки несостоятельности рынка

Позитивные или негативные экстерналии возникают тогда, когда решение, принятое одной из сторон, приносит выгоды или убытки другим сторонам, не имевшим в этом решении права голоса. Пусть, например, домовладелец перекрашивает свой дом ради собственного удовольствия. В результате во всем квартале становится приятнее жить, вплоть до того, что недвижимость в нем может даже вырасти в цене. С другой стороны, если дом покрасят в аляповатые цвета, эффект может оказаться противоположным. Так или иначе, домовладельцу нет никакого резона принимать эти эффекты во внимание – если только в районе не действуют правила или соглашения домовладельцев, которые способствовали бы возникновению позитивных экстерналий и избегали негативных.

Асимметрия информации возникает, когда одна из сторон знает о предмете сделки больше другой. Классический пример – рынок подержанных автомобилей. Продавец машины знает о ее качестве и истории больше покупателя. Однако владельцам хороших машин, объективно стоящих дороже, трудно убедить покупателей в их качестве, поэтому машины, одинаковые на бумаге (модель, год выпуска, пробег), продаются за одну и ту же среднюю цену. В результате чем лучше машина, тем труднее ее продать, и рынок насыщен плохими автомобилями – «лимонами». Дилер на вторичном рынке еще может создать себе репутацию, продавая отличные машины или давая покупателям гарантию для защиты их денег, но продавец с одной машиной репутации, скорее всего, не имеет, и средств на гарантию у него нет.

Асимметрия информации выливается в целый ряд последствий, из которых нам сейчас интересны два.

- Неблагоприятный отбор. Положение на рынке диктуют те, кто обладает большей информацией, потому что они могут выбирать свое участие. На рынке подержанных машин, поскольку способа продемонстрировать качество товара нет, продаваться будут только плохие машины, и рынок выродится в «рынок лимонов». На страховом рынке клиент знает свои риски лучше страховой компании, что тоже может привести к неблагоприятному отбору, поскольку клиенты с высокими рисками чаще страхуются (вследствие чего повышается риск для всего пула застрахованных, а следовательно, и стоимость страховки).

- Моральный риск. Страхование может привести к тому, что застрахованные начнут идти на больший риск, так как отвечают за свои действия уже не в полном объеме. Например, если бы автострахование покрывало любое повреждение автомобиля без учета франшизы и ответственности водителя, то у людей было бы меньше оснований аккуратно парковаться и даже аккуратно водить. Это и есть моральный риск.

Франшиза в автостраховании предусмотрена как раз для борьбы с асимметричной информацией. Во-первых, владелец автомобиля несет часть финансовой ответственности за свои действия, поэтому моральный риск ниже. Во-вторых, многие страховые компании борются с неблагоприятным отбором, предлагая разные типы сочетаний «страховая премия – франшиза». Автовладельцы, знающие, что для них риск низок, выбирают низкую страховую премию и высокую франшизу, зная, что, скорее всего, им ее платить не придется. Автомобилисты с высоким риском выбирают более высокую премию и низкую франшизу, которую уже рассчитывают заплатить.

В ряде случаев проблему неблагоприятного отбора индустрия может решить сама, как в автостраховании, но в других ситуациях может потребоваться государственное регулирование. Например, в медицинском страховании человек знает о себе больше, чем страховая компания – и о своей медицинской истории, и о наследственности, и об образе жизни (хотя сейчас, с появлением фитнес-трекеров, дешевых тестов ДНК и оцифровкой историй болезни, это может и измениться). В результате неблагоприятного отбора медстраховку чаще приобретают те из нас, кто больше рискует, повышая тем самым ее стоимость. Одна из множества причин, по которым государства регулируют здравоохранение (как в Великобритании) или требуют от каждого приобрести частную медстраховку (как в Швейцарии), в том и заключается, чтобы охватить страхованием более широкий и здоровый спектр населения и тем самым снизить стоимость страховки.

Три типа атрибутов в экономике у продукта или услуги касательно асимметричной информации

Аналогичные проблемы возникают и с кибербезопасностью: частный рынок может помочь в поиске решений для борьбы с асимметрией информации, но в ряде случаев может потребоваться вмешательство государства.

Аспекты асимметричной информации

Проблемы с оценкой качества подержанной машины очевидны, но даже для нового автомобиля имеется огромная масса асимметричной информации, задействованной в принятии решения о покупке. Проблему оценки качества подержанной машины легко понять, но даже для новой имеется множество неопределенностей. Здесь есть много атрибутов, связанных с разной степенью информационной асимметрии, и несколько способов проверить

истинность таких атрибутов. Во-первых, покупка начинается с принятия решения о том, какой тип машины купить. Даже для новой машины встает вопрос качества, в дополнение к расходу топлива и безопасности. Некоторые из этих атрибутов ясны сразу, а другие могут не проясниться никогда.

Как же мы принимаем решение?

Первое, что выбирают многие из нас, – это тип автомобиля: кому-то нужно спортивное купе, а кому-то микроавтобус на семь пассажиров с большим грузовым отсеком, и эти атрибуты у любого автомобиля четко видны. Другие детали выяснить труднее – например, насколько машина легка в управлении и сколько она пробегает, пока не развалится. Первое легко выяснить с помощью тест-драйва, а мнение о качестве мы можем составить по репутации фирмы-изготовителя. И, наконец, мы никак не можем заранее проверить подушки безопасности, расход топлива, уровень выбросов или прочность кузова при аварии. Здесь людям может потребоваться положиться на третью сторону, например, на государство, которое проводит испытания и допускает машины к продаже при соблюдении минимальных стандартов.

В экономике у продукта или услуги касательно асимметричной информации есть три типа атрибутов:

- ПОИСКОВЫЕ - атрибуты, которые можно оценить заранее, такие как тип машины.
- ОПЫТНЫЕ - атрибуты, проявляющиеся лишь с течением времени, такие как качество машины.
- ДОВЕРИТЕЛЬНЫЕ - атрибуты, которые могут никогда не стать известными, такие как качество подушки безопасности.

Было разработано несколько моделей для помощи в оценке этих атрибутов, и, как правило, они включают привлечение третьей стороны для тестирования, сертификации или государственного регулирования одного или нескольких атрибутов.

Рейтинги

Доверенные независимые агенты могут испытывать продукты и услуги на наличие тех или иных атрибутов, предоставляя потребителям рейтинги в качестве информации перед покупкой. Например, журнал Consumer Reports (http://www.consumerreports.org) оценивает большое количество продуктов по широкому спектру атрибутов. Для автомобилей проверяется безопасность, надежность и общая удовлетворенность потребителя.

Сертификация

Для некоторых атрибутов рейтинг не нужен, а требуется лишь подтверждение того, что продукт соответствует некоему стандарту приемлемости. Например, UL (бывш. Underwriters Laboratories, http://www.ul.com/) – это частная компания, которая может сертифицировать соответствие качества продукции, например, электротоваров, своим собственным стандартам. В автопромышленности производители автомобилей в некоторых странах могут самосертифицировать некоторые атрибуты, такие как экономия топлива или экологичность выбросов, что недавно выявило потребность в независимых экспертах.

Государственное регулирование

Оценить доверительные атрибуты, такие как безопасность, ни потребитель, ни частная независимая сторона не могут. Поэтому может потребоваться, чтобы стандарты безопасности проверяло государство. Например, государство может проводить краш-тесты автомобилей и проверять их на соответствие стандартам безопасности.

Вернемся к безопасности данных: асимметрия информации затрудняет потребителям оценку безопасности данных по различным атрибутам. Поэтому организациям нужно как-то подавать надежные сигналы своего уровня безопасности. Способы сделать это с привлечением третьих сторон обсуждаются в разделе рекомендаций.

Выводы

Экономика утечек данных позволяет вычленить ряд важных аспектов борьбы с ними.

Во-первых, организации должны нести ответственность за негативные экстерналии – убытки, понесенные в результате их действий другими организациями, пользователями и обществом в целом. Во многих случаях такая ответственность может быть финансовой – подобно налогообложению тех или иных типов загрязнения. Повышение ответственности или штрафы за допущение утечек, несомненно, снизят вероятность их возникновения. И точно так же, как некоторые виды загрязнения (например, свинец в краске или бензине) настолько опасны, что их приходится явно запрещать, может потребоваться законодательно закрепить те или иные меры безопасности.

Во-вторых, для борьбы с асимметрией информации следует сделать ее более симметричной. Если организации могут убедительно продемонстрировать свой уровень кибербезопасности потребителям, они будут охотнее инвестировать в нее, так как инвестиции окупятся. Это оживит рынок страхования кибербезопасности, а также снизит уровень морального риска, так как компании с лучшими практиками окажутся в более выгодном положении. В конечном счете, выиграет потребитель, так как организации, с которыми он взаимодействует в Интернете, будут заинтересованы в укреплении безопасности данных.

Эти рекомендации мы подробнее рассмотрим в статье "Утечки данных. Рекомендации" в разделе Безопасность.

Источник: Global Internet Report 2016, https://www.internetsociety.org/globalinternetreport/2016/

Распределение хранилищ данных по регионам

369GB

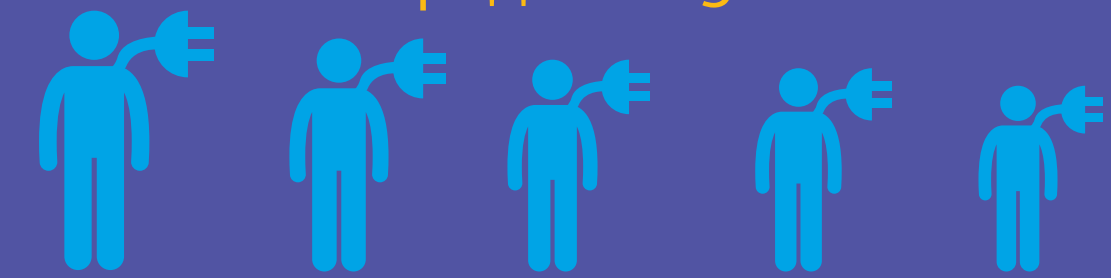
В целом

На душу населения

Передовые/отстающие 5 на 2012 *

*на основании 48-ми стран

Передовые 5



2,331GB Швейцария

2,095GB Дания

2,031GB Норвегия

2,024GB ГонгКонг

1,977GB Америка

Отстающие 5

245GB Турция

156GB Вьетнам

134GB Филиппины

120GB Индонезия

64GB Индия

Топ-10 стран

Общий объем установленных носителей (Все типы носителя)

Рейтинг	2000	2005	2012
1	Америка	Америка	Америка
2	Япония	КНР	КНР
3	Германия	Япония	германия
4	КНР	Германия	Япония
5	Великобритания	Великобритания	Великобритания
6	Франция	Франция	Бразилия
7	Корея	Италия	Франция
8	Италия	Бразилия	Индия
9	Канада	Корея	Россия
10	Австралия	Канада	Корея

Рейтинг стран по отношению к общему объему установленных носителей

Типы носителей


HDD


Tape


Optical

Flash


DRAM

ОБЩИЙ ОБЪЕМ ХРАНИЛИЩ ДАННЫХ В МИРЕ

Источник:
http://www.idc.com/downloads/where_is_storage_infographic_243338.pdf

Структурный разбор данных SDN: Все дело в аналитике

Ченгиз Алаэттиноглу (Cengiz Alaettinoglu)*

Поставщики услуг вынуждены управлять все более сложными сетями для поддержки сразу нескольких сервисов с различными и часто взаимоисключающими потребностями. Также им приходится обрабатывать все большее количество все более частых запросов к ресурсам сети, предоставляя нужные ресурсы за считанные секунды. Эксплуатировать сети такого размера и сложности, как сейчас, силами одних только инженеров невозможно. Технологии виртуализации сети и SDN позволяют строить динамические, гибкие сети IP/MPLS, которые можно быстро переконфигурировать для адаптации к новым бизнес-требованиям. Однако для того, чтобы сделать автономные сети реальностью, им не хватает управленческого интеллекта.

Программно-определяемые сети (Software-defined networking, SDN) революционизируют сети дата-центров, разделяя уровни управления и уровни данных, а также позволяя приложениям программировать уровень управления. Сейчас мы наблюдаем высочайший уровень инноваций в сетевых приложениях для дата-центров: от оверлеев виртуальных сетей до систем безопасности. Программно-определяемые WAN (SD-WAN) используют этот подход на границе сети, реализуя интеллектуальный метод перенаправления критически важного трафика WAN по дорогостоящим контурам MPLS, а некритичного трафика – по менее дорогим интернет-каналам.

Следующим этапом эволюции SDN станет применение этой архитектуры к WAN (Wide Area Network, территориально-распределенная сеть) и решение проблем с управлением, стоящих перед операторами. В отличие от SD-WAN, WAN-SDN (также называемые Carrier SDN) распространяют принцип программно-определяемой сети и на базовую сеть. Для поставщиков услуг это магистральная сеть или городская сеть. Для крупных предприятий, не отдающих свою сеть IP/MPLS на аутсорсинг, это WAN. В этой статье мы будем рассматривать WAN-сети IP/MPLS поставщиков услуг.

Многие из поставщиков услуг делают ставку на технологии SDN, чтобы создавать динамичные, гибкие сети, которые можно быстро перенастраивать для реализации новых бизнес-требований. Автоматизация обеспечения связности и активации услуг дает убедительные преимущества, включая возможность предлагать больше услуг и получать большую отдачу от капиталовложений, сокращение срока окупаемости и повышение эффективности операций.

Однако одна лишь автоматизация не позволит поставщикам услуг выполнить свои бизнес-задачи. SDN создают множество управленческих проблем, включая потерю прозрачности и контроля над изменениями в сети, а также необходимость реализовать инженерные ноу-хау в приложениях SDN.

Для создания сетей, адаптирующихся к бизнес-потребностям, поставщикам услуг необходима аналитика SDN для планирования в реальном времени и повышения видимости сервисов в сетевых инфраструктурах как традиционного вида, так и с поддержкой SDN. Для получения этой аналитики и создания подлинно адаптивных сетей требуется еще один уровень менеджмента. В настоящей статье мы рассмотрим проблемы, встающие перед поставщиками услуг, особенности SDN-аналитики и некоторые примеры практической реализации.

Проблемы мультисервисных сетей

Сети современных поставщиков услуг очень сложны, так как должны поддерживать множество приложений и сервисов сразу – доступ в Интернет, потоковое видео, VoIP, VPN уровней 2 и 3, мобильные транспортные сети связи 3GPP и базовые транспортные магистрали, облачные сервисы и многое другое. А ведь в прошлом, как правило, для разных приложений выделялись разные сети. Например, у провайдера могла быть сеть Frame Relay для корпоративных клиентов, городская сеть на основе кольца SONET для мобильной транспортной сети связи, сеть с негарантированной доставкой для доступа в Интернет и так далее.

Очевидно, что эксплуатация нескольких сетей требовала больших капитальных и операционных издержек, чем содержание одной многосервисной сети. Кроме того, многие традиционные сети использовали технологии коммутации каналов и трудно и дорого масштабировались, поскольку выделенная, но неиспользуемая мощность

пропадала зря. Теперь многие приложения работают в виде сервисов поверх конвергентных сетей IP/MPLS с коммутацией пакетов, которые гораздо более эффективны, масштабируемы и терпимы к сбоям. Однако их быстродействие менее предсказуемо и требует внимательного мониторинга сервисных маршрутов.

Поддержка уникальных требований сервисов

Развертывание нескольких приложений в конвергентной сети поднимает ряд проблем с управлением, так как у каждого из приложений свои требования к быстродействию, своя скорость роста и своя устойчивость к сбоям. Например, финансовая организация может быть готова платить дополнительно за маршруты с очень малой задержкой, чтобы поддерживать свое трейдинговое приложение. Для этого поставщику услуг может потребоваться найти эти маршруты с малой задержкой, отделить трафик приложения от остального трафика и полностью защитить его от сбоев каналов и маршрутизаторов.

В то же время у сервисов потокового видео сверхвысокого качества для домашних пользователей (таких, как Netflix и YouTube) высокие требования к качеству, и их невыполнение приведет к пикселизации, задержкам воспроизведения и в итоге к уходу клиентов. Поэтому для такого трафика лучше всего маршруты с низкой вариацией задержки. Потоковое видео адаптируется к доступной полосе пропускания в известных пределах, поэтому оператор может при нормальных условиях предоставлять оптимальное качество видео, но разрешить его снижение до приемлемого уровня во время пиковой нагрузки или при сбое.

Кроме поддержки нескольких сервисов, перед поставщиками услуг встает еще одна проблема – увеличение частоты запросов на активацию/деактивацию сервисов вместе с сокращением приемлемого времени провизионирования : от недель до часов и даже секунд. Например, многие провайдеры предлагают клиентам порталы самообслуживания, где они могут запросить дополнительную пропускную способность.

Необходимость автоматизации

Оптимизация сети для любого сервиса сложна и требует значительных затрат труда высокооплачиваемых инженеров. Такой подход не масштабируется. Например, рассмотрим время на оптимизацию трафика того или иного приложения. Как правило, создается матрица спроса на трафик, где сопоставляется объем входящего трафика на каждом входном маршрутизаторе и на каждом выходном маршрутизаторе, через который трафик покидает сеть. Потом на основе этой матрицы и топологии сети применяется алгоритм оптимизации, выдающий рекомендуемые маршруты для каждой пары «вход-выход» в матрице трафика, чтобы свести к минимуму максимальную нагрузку на каналы в сети. После вычисления маршрутов они провизионируются в сетевых устройствах.

Теперь, со смещением фокуса в сторону сетей IP/MPLS, работать вручную стало невозможно. Раньше IP/MPLS использовался на магистральных линиях сети и число маршрутизаторов не превышало, скажем, 500. С ростом трафика, в частности, трафика мобильных пользователей, поставщики услуг были вынуждены распространить IP/MPLS на сети доступа и агрегирования.

В результате количество маршрутизаторов, которыми поставщик услуг должен управлять, возросло в разы, иногда достигая 20 тысяч. Эксплуатация сети IP/MPLS такого размера – сложнейшая задача. Например, у провайдера среднего размера единовременно могут «лежать» 5% туннелей, используемых для инжиниринга трафика. Но это больше 1000 туннелей! Если инженеры будут вручную определять причины простоя туннелей, об оперативности не может быть и речи – процесс займет несколько часов или даже дней. Хуже того, к тому времени, когда анализ закончится, данные устареют, потому что сеть уже изменится.

Поэтому оптимизация мультисервисной сети вряд ли возможна без автоматизации. SDN поможет решить эти проблемы и упросить провизионирование сетей. На рис. 1 показана простая двухуровневая архитектура, где приложения SDN контролируют поведение сети. Сетевые устройства (физические и виртуальные) не конфигурируются. Вместо этого они программируются с помощью нисходящих программных интерфейсов (API) одним или несколькими контроллерами SDN или оркестраторами сервисов, выполняющими высокоуровневые функции планирования между доменами, а иногда и между IP/MPLS и оптикой. Контроллеры предоставляют доступ к приложениям посредством восходящих API, позволяя приложениям модифицировать поведение сети под собственные нужды.

Важность аналитики SDN

Хотя контроллеры SDN дают возможность менять конфигурацию сети программно, им явно недостает управленческого интеллекта. Если приложения и сервисы развертываются без участия оператора и при недостаточной прозрачности, как же их можно планировать? Кто (или что) решает, следует ли применять эти программные изменения? Как оператор знает, что сеть вообще способна поддерживать новый запрос, не поставив под угрозу работу существующих приложений?

На эти вопросы отвечают программы аналитики. При использовании SDN программное обеспечение должно обладать теми же самыми ноу-хау, что и живые инженеры. По сути, это та же автоматизация, которая осуществляется уже много лет, только в несравнимо большем масштабе. Аналитика SDN – обогащенная и направляемая человеческим разумом – может вычислять воздействие требуемых изменений и принимать решения о том, можно ли их допустить или нет.

Телеметрия и аналитика

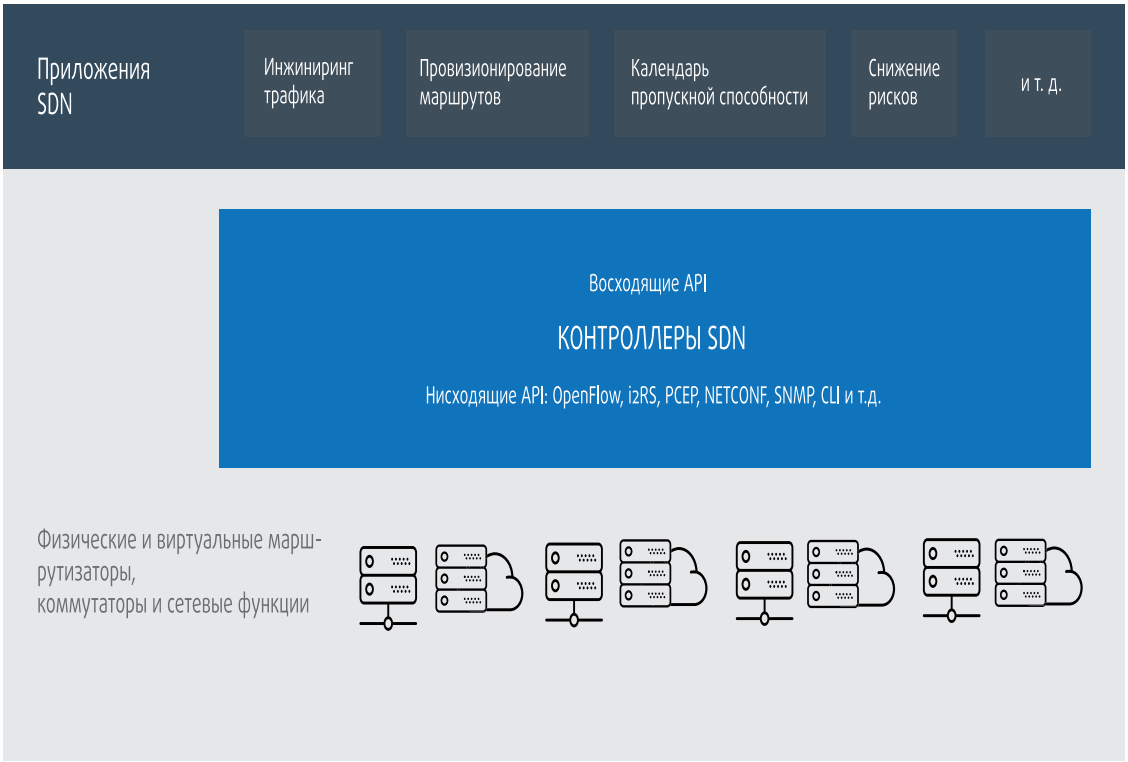
Многие в индустрии говорят о телеметрии, которая совершенно необходима, но все же отличается от аналитики. Управление SDN требует множества данных о том, что происходит в сети, в частности, о топологии IGP, маршрутах BGP, правилах брандмауэров, требованиях трафика, задержках и их вариации, быстродействии, загрузки интерфейсов и т.д. Эти данные необходимы, но их недостаточно. Телеметрия – всего лишь сбор этих данных, то есть лишь начало эффективного управления SDN.

Аналитика – получение из этих данных выводов, на основе которых можно действовать. Аналитика, в частности, позволяет определить, что именно не в порядке с сетью, и предложить варианты исправления ситуации. Многие проекты больших данных просто топят инженера в них, не говоря, что с ними делать дальше.

Функции аналитики SDN

Аналитика SDN несет две важных функции. Первая из них – поддерживать прозрачность управления сетью, даже если изменения в ней делаются программно. В отсутствие традиционного процесса постановки задач операторы могут просто не

Рис. 1. Двухуровневая архитектура WAN-SDN.



знать об изменениях. До тех пор, пока программные изменения работают и дают желаемые результаты, такая непрозрачность может быть приемлемой. Но когда изменение становится проблематичным, как оператор может диагностировать проблему или найти «ответственное» за нее приложение, забагованный контроллер или неисправное сетевое устройство?

Аналитика SDN должна обеспечивать прозрачность сети – устройств и контроллеров, – регистрируя данные телеметрии в реальном времени, поступающие с уровней управления и данных в сети, в том числе топологию маршрутов, метрики быстродействия и данные потоков трафика. Зарегистрированные данные могут быть очень полезны при разборах инцидентов постфактум для определения основополагающих причин.

Вторая, еще более важная функция аналитики SDN, – это интеллектуальное управление. Аналитика SDN жизненно важна для таких задач, как:

- устранение неполадок и визуализация;
- определение состояния сети в любой момент времени;
- инспекция и воспроизведение событий, информация о которых получена с контроллера и сетевых устройств;
- сравнение состояния маршрутизации и маршрутов для ситуаций, когда сервис/приложение работает хорошо и плохо;
- мониторинг маршрутов на предмет изменения в количестве сегментов, метрики, задержки и полосы пропускания.

Например, традиционно, когда оператору требуется внести существенные изменения в сеть, создается группа планирования, оценивающая готовность сети к таким изменениям. Когда поставщик услуг получает нового корпоративного клиента, либо когда предприятие развертывает новый сервис, группа планирования должна определить, достаточно ли у сети для этого мощностей. Если ответ отрицательный, группа планирования пытается найти в сети маршруты, которые могут удовлетворить новые потребности.

Для того, чтобы программируемое планирование SDN было жизнеспособно, ноу-хау планирования, применяемые в практике такой работы, должны быть воспроизведены в аналитическом ПО. Как только программа выдает решение, контроллер или оркестратор SDN может провизионировать его в сети. Такая аналитика делает возможным управлять значительно более крупными сетями за счет автоматизации. Разумеется, аналитическое ПО не может принимать правильные решения без данных телеметрии о каждом аспекте сети.

Место для аналитики

Чтобы аналитика была жизнеспособной, необходимо подобрать ей правильное место в архитектуре SDN. Это место – не в устройствах. Четыре-пять лет назад индустрия полагала, что аналитику стоит размещать в контроллере. Этого не случилось. Во-первых, контроллеры подешевели и в чем-то упростились. Изготовители отвели аналитике место дополнительной платной функции и стали реализовывать ее лишь в наиболее продвинутых продуктах своих линеек.

Во-вторых, контроллер - это устройство уровня управления. Поставщикам услуг нежелательно осуществлять работу с большими данными в контроллерах. Аналитику можно размещать в приложениях (например, для инжиниринга трафика), но здесь возникает та проблема, что не у всех приложений есть доступ к одной и той же телеметрии. Одно приложение не знает, что происходит в другом, другое – в третьем, и так далее.

Следовательно, аналитику следует размещать на отдельном уровне над уровнем управления. Поэтому в архитектуру SDN добавлен новый уровень: аналитики и автоматизации. Так что, с учетом важности аналитики SDN, двухуровневую архитектуру SDN с рисунка 1 необходимо расширить, включив в нее основанный на аналитике уровень планирования, как показано на рисунке 2. Этот новый уровень реализует как прозрачность управления, так и интеллект для приложений SDN.

Поскольку SDN создает новые проблемы управления, необходимо переоценить и обновить традиционные управленческие процессы и инструменты. Например, если программные изменения в сети происходят каждые несколько минут или секунд, то периодический сбор данных метрики путем опроса устройств становится неприменим, как и использование только данных потока. Развертывание датчиков для мониторин-

га постоянно изменяющихся виртуальных устройств и сервисного трафика дорого и проблематично. В динамических сетях требуется телеметрия и аналитика в реальном времени, основанная на push-опросах.

Применение аналитики SDN

Поставщики услуг все время находят новые возможности применения SDN. Приведем несколько примеров использования SDN и продемонстрируем на них всю важность аналитики.

Быстрое провизионирование: радикальная оптимизация рабочего процесса. Одна из основных целей поставщиков услуг – сократить время создания и активации услуг с нескольких недель до нескольких минут. Организации могут достичь этой цели, устранив трудоемкое ручное планирование для таких задач, как инжиниринг трафика, и автоматически генерируя рекомендации по оптимальной конфигурации сети.

Увеличение КПД сетей: традиционно, сети поставщиков услуг работают при нагрузке на каналы примерно 45%. Это дает достаточный запас прочности на случай аварии. Но это же означает многомиллионный мертвый капитал. Один из методов снижения затрат, что является приоритетной целью для многих поставщиков услуг, – это повышение нагрузки на каналы, что позволит получить большую отдачу от уже сделанных капиталовложений в инфраструктуру сети и даст экономию на дополнительных капитальных издержках.

Для многих поставщиков услуг конечной целью является доведение нагрузки на каналы до 70%. SDN может сделать эту цель реальной благодаря самооптимизируемым, самовосстанавливаемым сетям. Однако высокая нагрузка достижима только при наличии аналитики, как в реальном времени, так и прогностической, которая управляла бы сетевой конфигурацией, успевая за изменяющимися потребностями. Например, поведение сети в условиях аварии можно предсказать на основе исторических данных о состоянии сети и моделирования. Развернув контроллеры SDN, управляемые таким интеллектом, поставщики услуг могут быть уверены, что никакие автоматические изменения не сорвут работу приложений и сервисов, даже в аварийных условиях.

Многоуровневая оптимизация: поставщики услуг желают использовать технологию SDN для того, чтобы объединить управление и планирование уровней IP/MPLS и оптического транспортного уровня. Это позволит операторам оптимизировать инжиниринг трафика, учтя показатели быстродействия, защиты и стоимости для каждого уровня. Операторы получат гибкий пул ресурсов, которые смогут автоматически и интеллектуально реагировать на изменение состояния сети и бизнес-требований.

Восстановление после аварий: при возникновении аварии с точки зрения SDN поставщик услуг должен быстро восстановить их предоставление и обеспечить соблюдение SLA. Для этого требуется понимание характера трафика – как в реальном времени, так и в прошлом – и того, как следует перенаправлять трафик в различных аварийных сценариях. У контроллеров SDN должен иметься источник интеллекта, который давал бы им инструкции по оптимальному перенаправлению трафика в таких ситуациях, с тем чтобы альтернативные маршруты не перегружали другие приложения и сервисы.

Инжиниринг трафика: поставщики услуг желают автоматизировать сложную и трудоемкую задачу балансировки сетевой нагрузки IP/MPLS, чтобы свести к минимуму нагрузку на слабейшее звено, ликвидировать перегрузки сети и перенаправлять трафик в обход перегруженных каналов. Этого можно добиться посредством SDN, создавая туннели RSVP-TE (Resource Reservation Protocol) или SR-TE (Segment Routing) для перенаправления трафика с сильно перегруженных линий на слабозагруженные. В результате сетевые ресурсы в целом используются лучше, а сервисы предоставляются более надежно.

Для этого требуется такая аналитика, как матрицы трафика для различных сегментов сети, периодов времени и условий; моделирование маршрутов в реальном времени для прогнозирования эффекта изменений; алгоритмы оптимизации – все под управлением политик, определяемых пользователем.

Сервисы в разное время суток: Поставщики услуг предоставляют несколько сервисов, перепровизионируя сети в расчете на пиковый трафик. Вместо этого можно, используя прогностическую аналитику на основе исто-

Рис. 2. Трехуровневая архитектура WAN-SDN.

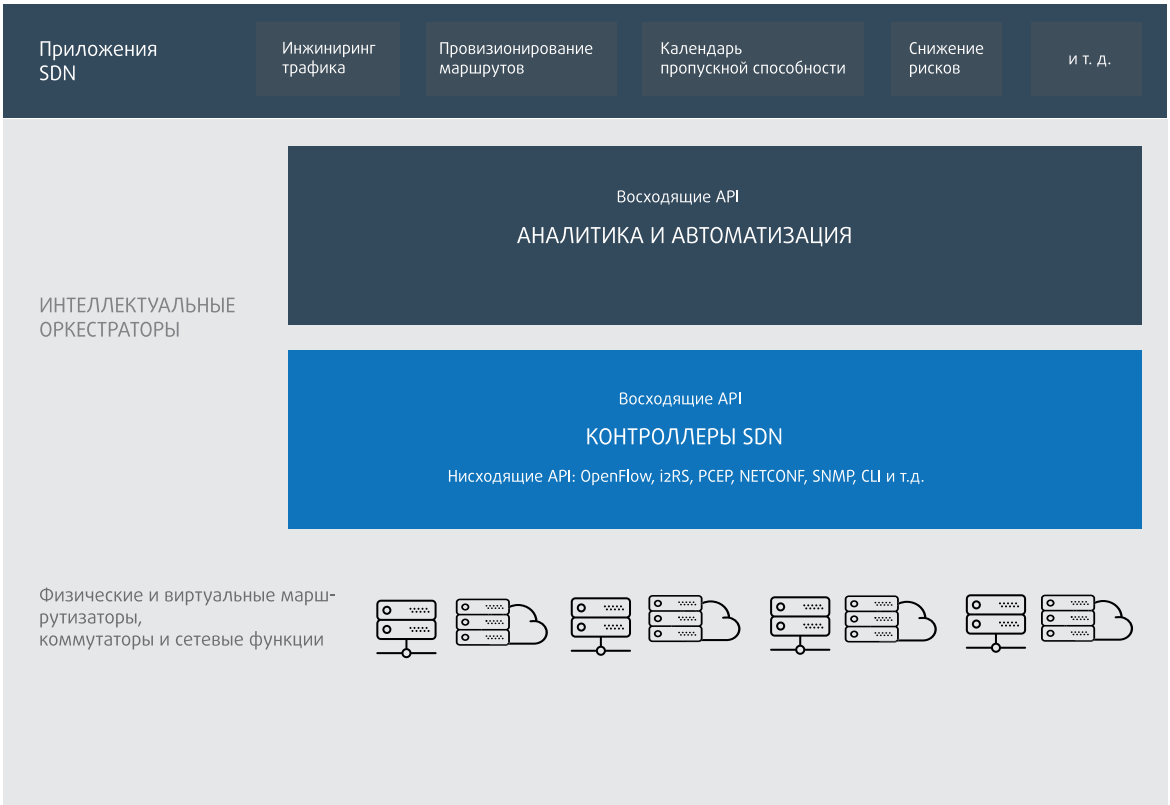
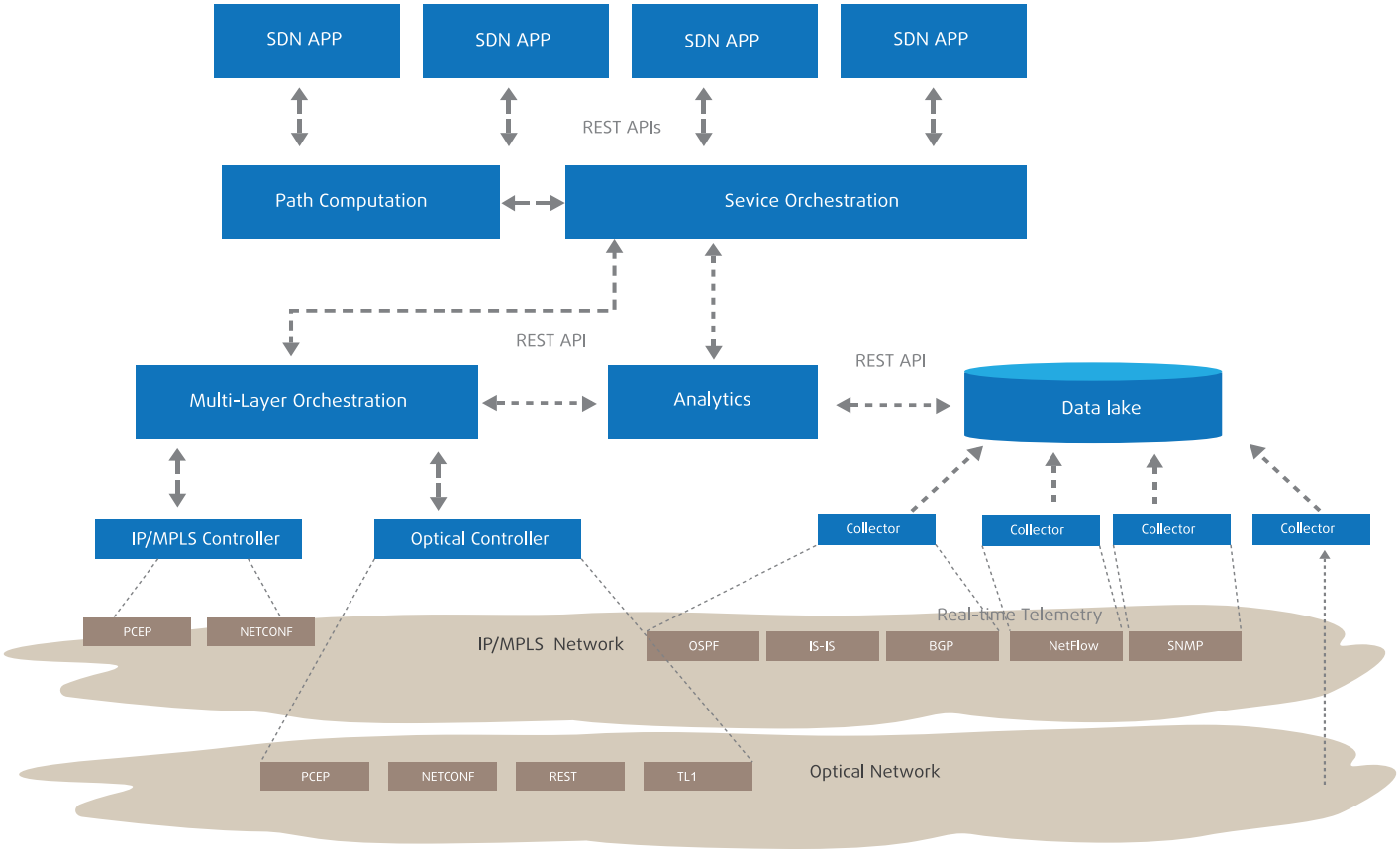


Рис. 3. Типичная многодоменная, многоуровневая, мультивендорная архитектура WAN-SDN.



рических моделей, оптимизировать сети в расчете на несколько пиков в день или неделю и минимизировать дополнительные капитальные издержки. Например, сеть можно оптимизировать для корпоративной сети в рабочее время и для потокового видео в нерабочее.

Гибридные облака: для эффективного использования ресурсов WAN и поддержки новых сервисов, таких как облачное резервное копирование или аварийное восстановление центров данных, требуется предоставление полосы пропускания по запросу и календарное планирование. Для этого необходимо регистрировать данные маршрутизации, трафика и быстродействия сети и создавать их базовые модели, чтобы подавать их на вход алгоритмов машинного обучения, рассчитывающих оптимальные сетевые конфигурации.

Суверенитет данных: многие организации в мире требуют, чтобы их данные не пересекали государственных границ. Это делается либо для выполнения законодательных требований, либо для соблюдения строгих внутренних политик безопасности, либо для того и другого сразу. Поставщикам услуг требуется создавать политики, явно определяющие устройства и каналы, по которым может проходить трафик, как на уровне оптики, так и на уровне IP-адресов. Необходимо знать, какие маршруты можно использовать, и иметь возможности для восстановления. Обычно это очень трудоемкий процесс. SDN делает возможными услуги защиты суверенитета данных, если у поставщика услуг есть интеллект, необходимый для автоматического обеспечения маршрутов.

Провизионирование VPN: VPN-сервисы являются важным источником дохода для многих операторов, и автоматизация провизионирования VPN, позволяющая ускорить их развертывание, является очень привлекательным направлением применения WAN-SDN. Однако не все VPN созданы равными: их требования к качеству обслуживания сильно различаются в зависимости от цели применения. Например, для репликации БД требуются маршруты с низкой задержкой; для гигантских потоков данных нужна большая полоса пропускания, где лучше всего подходит оптический уровень; для видео требуются маршруты с максимально стабильным пингом. Поэтому аналитика должна вычислить лучшие маршруты для каждого из этих сценариев, а также рассчитать воздействие новой VPN на другие услуги до автоматизации провизионирования.

Отвечать сложностью на сложность

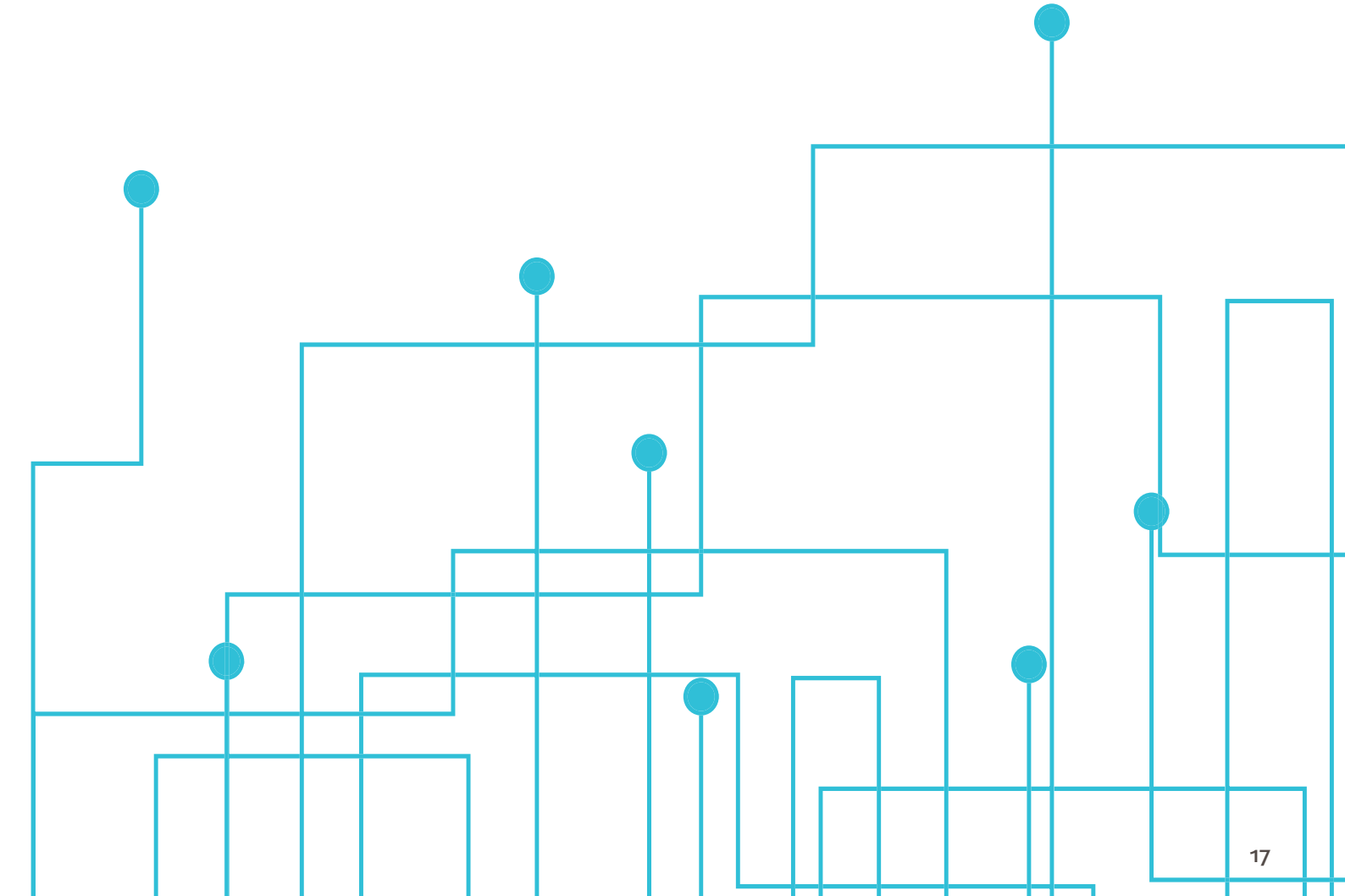
В силу сложности и важности сетей поставщиков услуг, где по всему стеку используется сразу несколько технологий, ни один вендор не может предложить полное решение. В самом деле, ранние архитектуры WAN-SDN, разрабатываемые и развертываемые поставщиками услуг, весьма сложны. Как правило, это многоуровневые, многодоменные экосистемы со множеством контроллеров и оборудованием от множества вендоров. Упрощенное представление такой архитектуры приведено на рисунке 3.

Тем выше потребность в открытых API для интеграции разнородных компонентов и в тесном сотрудничестве вендоров, ориентированном на удовлетворение потребностей заказчика. Например, в сценарии многоуровневой оптимизации возможность централизованного планирования сервисов, которое перенаправляло бы трафик на уровнях IP/MPLS и оптического транспорта, выполняя требования к стоимости и качеству обслуживания, становится реальностью благодаря сотрудничеству поставщиков электрического и оптического оборудования.

Итоги

Если поручить программе решения, традиционно принимавшиеся инженерами, такой программе необходимо передать все ноу-хау инженеров и сделать все изменения прозрачными для них. В динамических сетях требуется аналитика реального времени, управляемая корректными сетевыми данными. Их доставка должна осуществляться по уровню аналитики и автоматизации SDN между контроллером SDN и приложениями SDN. Только в этом случае поставщики услуг могут эффективно управлять своими мультисервисными сетями, повысить гибкость бизнеса, оптимально использовать свои капиталовложения и добавить новые возможности получения дохода.

Об авторе:
*Ченгиз Алаэттиноглу (Cengiz Alaettinoglu) – один из основателей научно-исследовательского подразделения компании Packet Design. Он отвечает за техническую стратегию разработки портфеля ее продуктов. Его ранние экспериментальные работы, посвященные анализу сходимости маршрутов и свойств масштабируемости, а также корреляции между быстродействием сети и инцидентами в работе протоколов маршрутизации, легли в основу технологии анализа маршрутов и портфеля продуктов Packet Design в целом. В настоящее время Ченгиз работает над созданием приложений для аналитики и планирования SDN в реальном времени с элементами искусственного интеллекта, которые смогут удовлетворять потребности в маршрутах и пропускной способности, не оказывая негативного влияния на другие сервисы. До прихода в Packet Design Ченгиз работал в Институте информационных наук Университета Южной Калифорнии, разрабатывая проект Routing Arbiter. Также он был сопредседателем рабочей группы IETF Routing Policy System, имеет большое количество публикаций и часто выступает на отраслевых мероприятиях по всему миру. Получил степень бакалавра (BS) по компьютерному инжинирингу в Ближневосточном техническом университете (Анкара), магистерскую и докторскую степени (MS и PhD) по компьютерным наукам в Университете штата Мэриленд.



Взаимодействие сетей доставки контента

Андрей Робачевский

Ценность данных или контента сегодня во многом определяется качеством доступа – насколько быстро загружается страница веб-сайта, насколько бесперебойно можно смотреть потоковое видео, насколько быстро реагируют интерактивные приложения. Сети доставки контента (Content Delivery Networks, CDN) являются ключевой платформой для достижения этих целей. Эффективность CDN во многом определяется тем, насколько близко точки ее присутствия находятся к потребителю контента. Возможность взаимодействия между CDN, возможность создания федераций открывают перспективное направление их развития в сторону увеличения охвата и уменьшения стоимости.

Ценность данных или контента сегодня во многом определяется качеством доступа – насколько быстро загружается страница веб-сайта, насколько бесперебойно можно смотреть потоковое видео, насколько быстро реагируют интерактивные приложения. Во многом – это ощущения пользователя. Быстрый сайт с хорошей реакцией подспудно является признаком качества предлагаемого материала, включая рекламу. И именно последняя играет существенную роль в желании провайдеров контента минимизировать задержки при доставке данных – если пользователь не может комфортно взаимодействовать с сайтом или рекламные вставки загружаются слишком долго, это ведет к реальным финансовым потерям.

По мере роста пропускной способности каналов и производительности серверов, казалось бы, эта цель будет достигнута естественным образом. Но, как мы знаем, Интернет по-прежнему не предоставляет никаких гарантий качества. Если пакет окажется утерян вследствие перегрузки какого-либо участка сети или доставлен с опозданием, вне изначального порядка, например, вследствие недоступности основного маршрута, задача приложений - обработать такие нерегулярности соответствующим образом. Пропускная полоса коммуникационного канала между приложениями также не гарантирована и заранее не известна. Она определяется множеством факторов, начиная от пропускной способности отдельных сегментов сетей, через которые передается трафик между приложениями, и заканчивая загрузкой самих сетей.

Поэтому для одного пользователя портал онлайн-магазина может загрузиться за 2 секунды, а для другого занять минуты, видеоролик вдруг внезапно замирает, пусть и на секунды, а повторяющиеся операции могут значительно различаться по времени.

Перефразируя известную поговорку, если пользователь не может забрать необходимый контент, контент должен быть доставлен пользователю! Так появилась идея сетей доставки контента – CDN (Content Delivery Networks) – наложенных сетей или еще одного приложения Интернета.

Эффективность CDN во многом определяется тем, насколько близко точки ее присутствия находятся к потребителю контента. Поэтому многие крупные CDN насчитывают десятки тысяч граничных серверов с глобальным покрытием. Например, на август 2016 года CDN компании Akamai насчитывала более 216 000 серверов, расположенных в 120 странах и работающих внутри более чем 1500 сетей. Но даже такая впечатляющая сеть не может покрыть весь Интернет. В то же время зоны покрытия существующих CDN имеют значительные перекрывающиеся области. Наконец, относительно небольшие CDN, чаще всего развернутые в рамках провайдера интернет-доступа или корпоративной сети, не могут достичь высокой эффективности в силу ограниченного покрытия.

Поэтому возможность взаимодействия между CDN, возможность создания федераций открывают перспективное направление их развития в сторону увеличения охвата и уменьшения стоимости. Рабочая группа IETF CDNI (Content Delivery Networks Interconnection, https://datatracker.ietf.org/wg/cdni/about/) занимается стандартизацией протоколов и документированием практики, необходимых для осуществления обмена данными между автономными CDN.

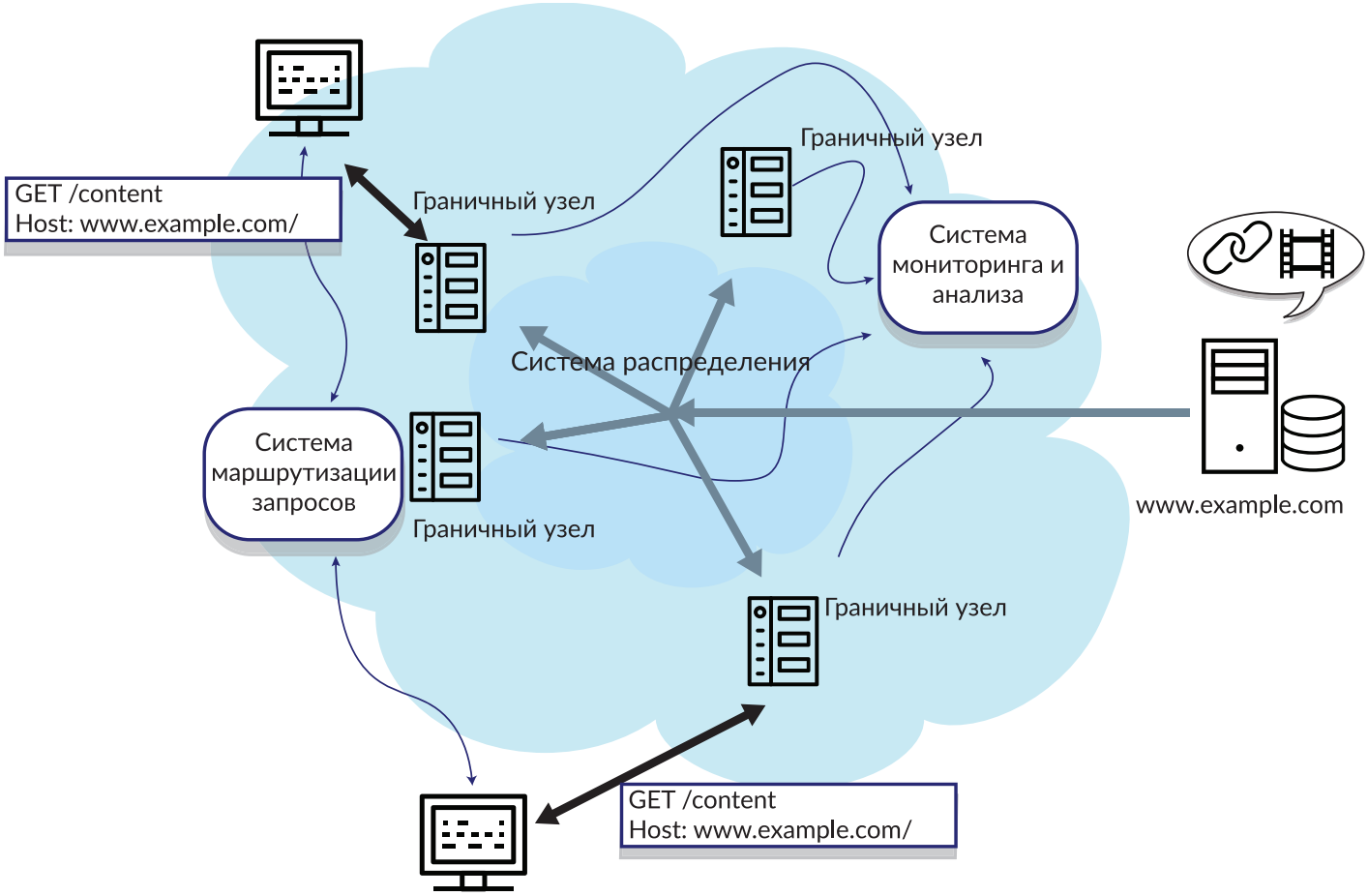
Но прежде чем более детально рассмотреть архитектуру CDNI, давайте кратко освежим в памяти, что же такое сеть доставки контента и зачем она нужна.

Как работает CDN

Идея CDN проста – разместить реплики контента как можно ближе к потенциальным его потребителям и тем самым обеспечить стабильную необходимую пропускную способность, а также распределить нагрузку на серверы, поставщики контента, например, на веб-серверы. Реализация этой идеи в глобальном Интернете гораздо сложнее и требует ответа на вопросы: где и сколько реплик должно быть размещено, как синхронизировать контент, каким образом осуществлять перенаправление запросов пользователя к нужной реплике?

Решение связанных с этими вопросами задач требует создания распределенной наложенной сети с функциями управления и мониторинга. Можно выделить следующие

Рис. 1. Основные компоненты CDN.



основные компоненты CDN, представленные на рисунке 1.

Граничные кэширующие узлы

Кэширующие узлы, объединенные в наложенную или выделенную сеть, обеспечивают доставку контента на «последней миле». От того, насколько географически распространена сеть и насколько «правильно» расположены граничные узлы, зависит общая производительность и качество CDN.

Граничные узлы могут представлять собой компьютерные кластеры для обеспечения надежности и распределения нагрузки. Обычно они размещаются вблизи точек обмена трафиком, где можно обеспечить связность CDN со множеством сетевых операторов. Иногда узлы могут быть размещены внутри сети, особенно в случае сети широкополосного доступа.

Запросы клиентов обслуживаются самими узлами локально, если запрашиваемые данные находятся в кэше. При их отсутствии данные копируются в кэш от сервера-источника. Однако кэширующие узлы отличаются от стандартного прокси, поскольку могут выполнять ряд других функций.

Управление кэшем

Различные классы контента требуют различных характеристик кэша. На основе статистической популярности и метаданных контента (например, заголовков Last-Modified) узел может вычислить возможное время истечения годность кэша и заранее освежить данные от источника. Это особенно важно в случае, когда сервер-источник не обеспечивает информацию по управлению кэшем (с помощью заголовков cache-control, etag, expires). Но даже если сервер использует заголовки для управления кэшем, они рассчитаны на кэширование браузером и не всегда адекватно работают в условиях CDN.

Поскольку CDN располагает значительной информацией относительно конкретного контента – его типа, характера запросов и т.п., управление кэшем может обеспечиваться более динамично, нежели с помощью заданных статических параметров кэша на сервере. Например, даже динамический контент, который обычно не подлежит кэшированию, имеет определенный период годности, в течение которого граничный узел может отвечать на запросы клиентов без обращения к серверу.

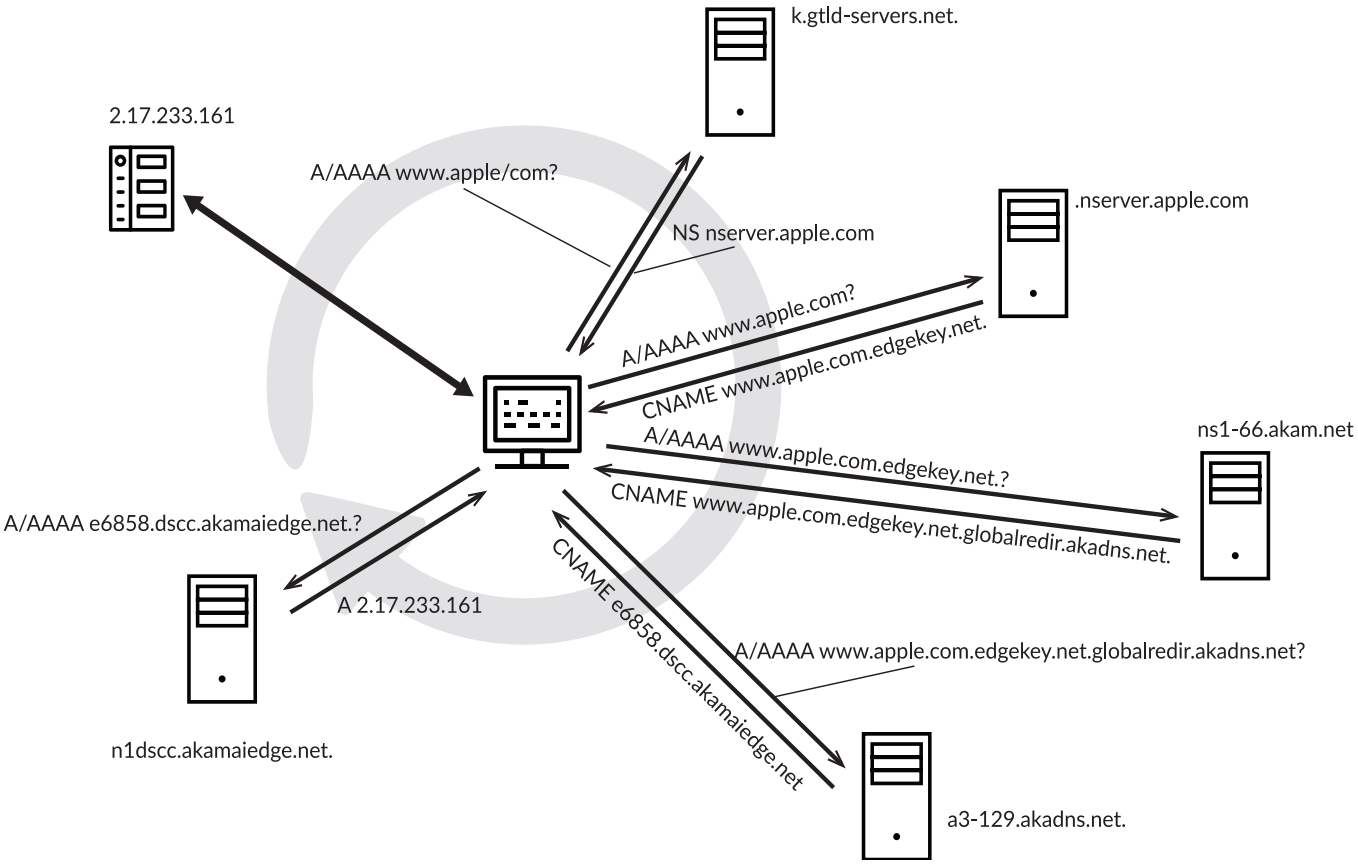
Определение местонахождения источника контента, включая обработку ситуаций недоступности

С помощью системы маршрутизации запросов, о которой мы поговорим далее, узел может принять решение о выборе наиболее оптимального экземпляра сервера-источника, о модификации запроса (модификация URL) или о перенаправлении запроса на другой граничный узел.

Изменение HTTP-заголовков

Граничные узлы могут добавлять, удалять или изменять заголовки HTTP-запросов и ответов, особенно заголовки куки (cookie), такие как set-cookie и cookie. Это может использоваться для обмена служебной информацией с сервером-источником и с пользователями, а также для управления каскадными кэшами.

Рис. 2. Каскадная трансляция имени www.apple.com для определения оптимального граничного узла.



Транспортная система доставки контента

В задачу транспортной системы входит оптимальная доставка требуемого контента к граничным кэширующим узлам. Небольшие CDN могут себе позволить одноуровневую структуру, когда граничные узлы посылают запросы на обновление кэша непосредственно веб-серверам. При этом для связности часто используется Интернет, а не выделенная сеть.

Крупные CDN используют многоуровневую структуру, когда группы граничных узлов приписаны к кэширующим кластерам более высокого уровня. Таким образом уменьшается нагрузка на веб-серверы – источники контента за счет увеличения частоты попадания в кэш (cache hit), а также уменьшается задержка доставки за счет дополнительного уровня распределения.

В качестве транспортной сети в крупных CDN используются либо наложенная, либо выделенная сеть. Во многих случаях используется оптимизация маршрутизации с использованием непрерывных тестов связности и пропускной способности между узлами. Все чаще для управления передачей трафика в транспортной сети используется архитектура SDN.

Более сложная структура иерархических кэшей используется при необходимости доставки видеопотоков, особенно в реальном времени. От граничных узлов также требуется дополнительная функциональность, так как они выполняют роль потоковых серверов. Потоковые серверы обеспечивают необходимую фрагментацию потока, его кодирование с различным разрешением/качеством и взаимодействие с клиентами.

Например, в сети Akamai в качестве узлов транспортной сети используется система «входных узлов» (entrypoint), расположенных в непосредственной близости к поставщику контента, и рефлекторов (set reflector), обеспечивающих оптимальную доставку данных в граничные узлы. Наконец, граничный узел представляет собой систему серверов, объединенных в мультикаст-сеть. Как и в обычной CDN, он обеспечивает доставку контента конечному пользователю.

Система маршрутизации запросов

Мозгом CDN является система маршрутизации запросов. В задачу этой системы входит выбор наиболее оптимального граничного узла для обслуживания запроса клиента. Выбор осуществляется на основе нескольких параметров, включая «близость» узла к клиенту, загрузку узла, наличие в кэше требуемого контента, а также других возможных правил (например, связанных с защитой авторских прав или доступности услуг в определенных географических областях).

Существует несколько методов маршрутизации запроса. Давайте рассмотрим основные из них.

Методы, основанные на использовании DNS

Эти методы являются наиболее популярными вследствие повсеместного присутствия DNS. В основе этого метода лежит использование специализированного DNS-сервера для трансляции имени ресурса, например, веб-сервера. В зависимости от указанных выше параметров выбора сервер возвращает различные записи ресурсов A/AAAA, CNAME или NS.

Так, например, в простейшем случае сервер может вернуть один или несколько IP-адресов оптимального граничного узла. Несколько IP-адресов позволяют осуществлять

простейшую балансировку загрузки, когда клиенты буду получать поочередно IP-адреса из множества, тем самым распределяя нагрузку среди нескольких граничных узлов.

В более сложных ситуациях может использоваться многоуровневая трансляция имени, позволяющая распределить процесс принятия решений по маршрутизации запроса между основным DNS-сервером и несколькими, более специализированным и обладающим более полной информацией, DNS-серверами. Для этого используются записи NS или CNAME.

Основным недостатком использования записи NS для «каскадирования» процесса трансляции является то, что число уровней ограничено числом частей самого DNS-имени. Например, имя a.b.example.com допускает лишь один уровень «каскадирования» от сервера, отвечающего за example.com к серверу, авторитетному за b.example.com, который, в свою очередь вернет IP-адрес a.b.example.com.

Поэтому наиболее распространенным является использование CNAME, которое не накладывает такого ограничения.

Например, для получения IP-адреса граничного узла CDN Akamai, обслуживающего сервер www.apple.com, клиенту необходимо обработать три перенаправления: сначала на www.apple.com.edgekey.net., затем на www.apple.com.edgekey.net.globalredir.akadns.net. и наконец, на e6858.dscc.akamaiedge.net., адрес которого укажет на оптимальный для клиента граничный узел. Этот процесс схематично представлен на рис. 2.

Как мы видим, DNS-серверы, осуществляющие эти перенаправления, на самом деле являются компонентами системы маршрутизации запросов и генерируют имена в соответствии с алгоритмом поиска оптимального граничного кэширующего узла.

Однако использование DNS для маршрутизации запросов имеет существенные ограничения.

Во-первых, маршрутизация происходит на уровне запрашиваемого доменного имени, хотя предпочтительней была бы маршрутизация на уровне запрашиваемого объекта. Например, объекты контента с различными характеристиками (размер, частота обновления, транспортные характеристики) могут быть размещены на различных кэширующих узлах. И в то же время все они могут быть адресованы различными URL с общим доменным именем.

Во-вторых, для определения местонахождения клиента используется IP-адрес DNS-резолвера клиента, а не самого клиента, поскольку DNS-запрос на трансляцию имени поступает именно от резолвера. В некоторых случаях это может привести к существенным ошибкам в определении «ближайшего» граничного узла. Особенно когда используются резолверы, расположенные вне сети клиента, например, общедоступные резолверы PublicDNS или OpenDNS.

Для решения этой проблемы в IETF недавно был документирован механизм (RFC7871 “Client Subnet in DNS Queries”, https://tools.ietf.org/html/rfc7871), позволяющий резолверу при обращении к авторитетному DNS-серверу указать префикс сети клиента (обычно /24 в случае IPv4). Для передачи этой информации используется специальная опция механизма расширений DNS EDNS0. Крупнейшие общедоступные резолверы PublicDNS (Google) и OpenDNS (Cisco), как и растущее число CDN, поддерживают эту опцию.

Тем не менее, проблема отчасти остается, как, впрочем, и проблема недостаточ-

Рис. 3. Структура взаимодействия двух CDN в рамках модели CDNI.

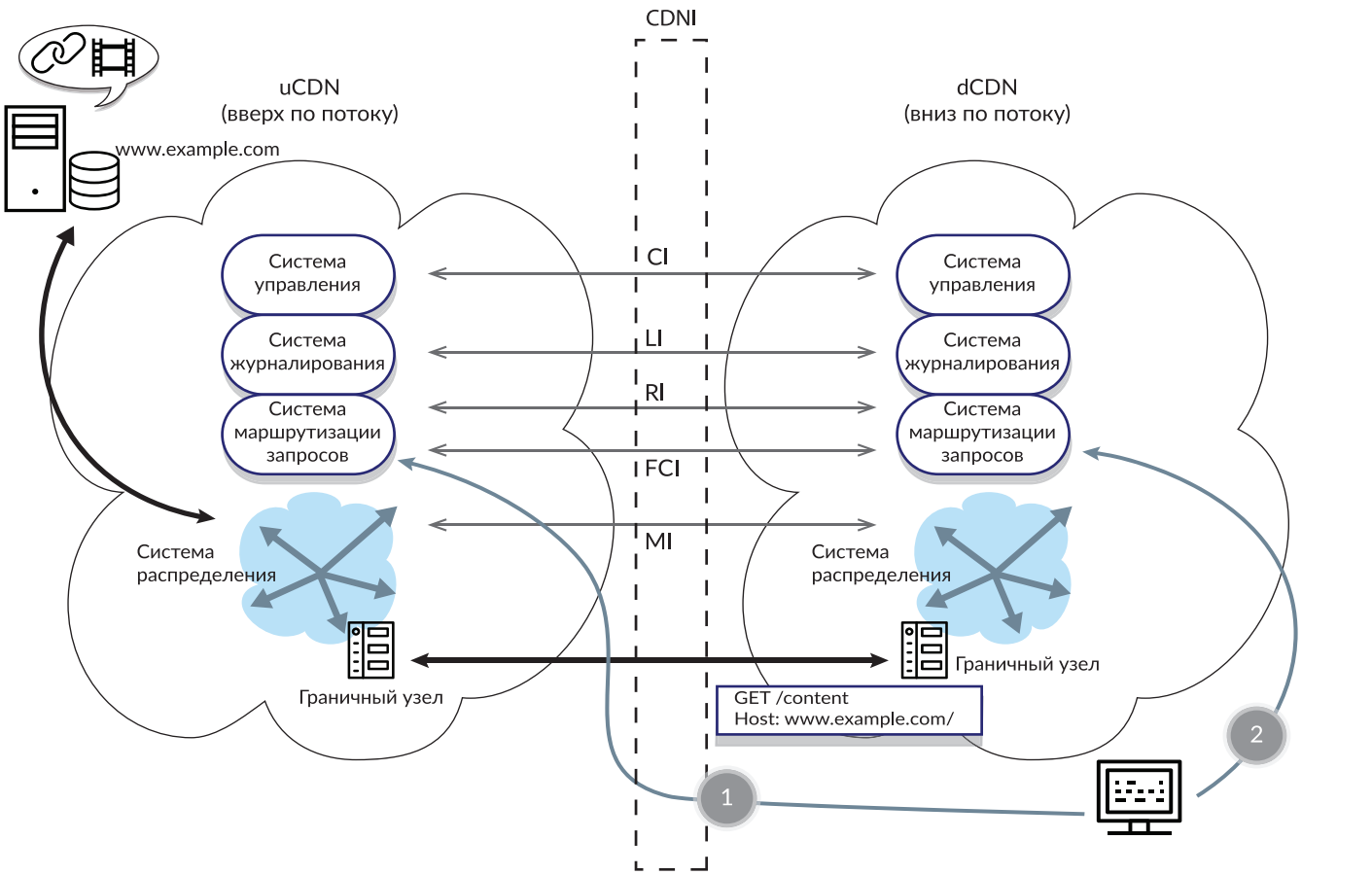
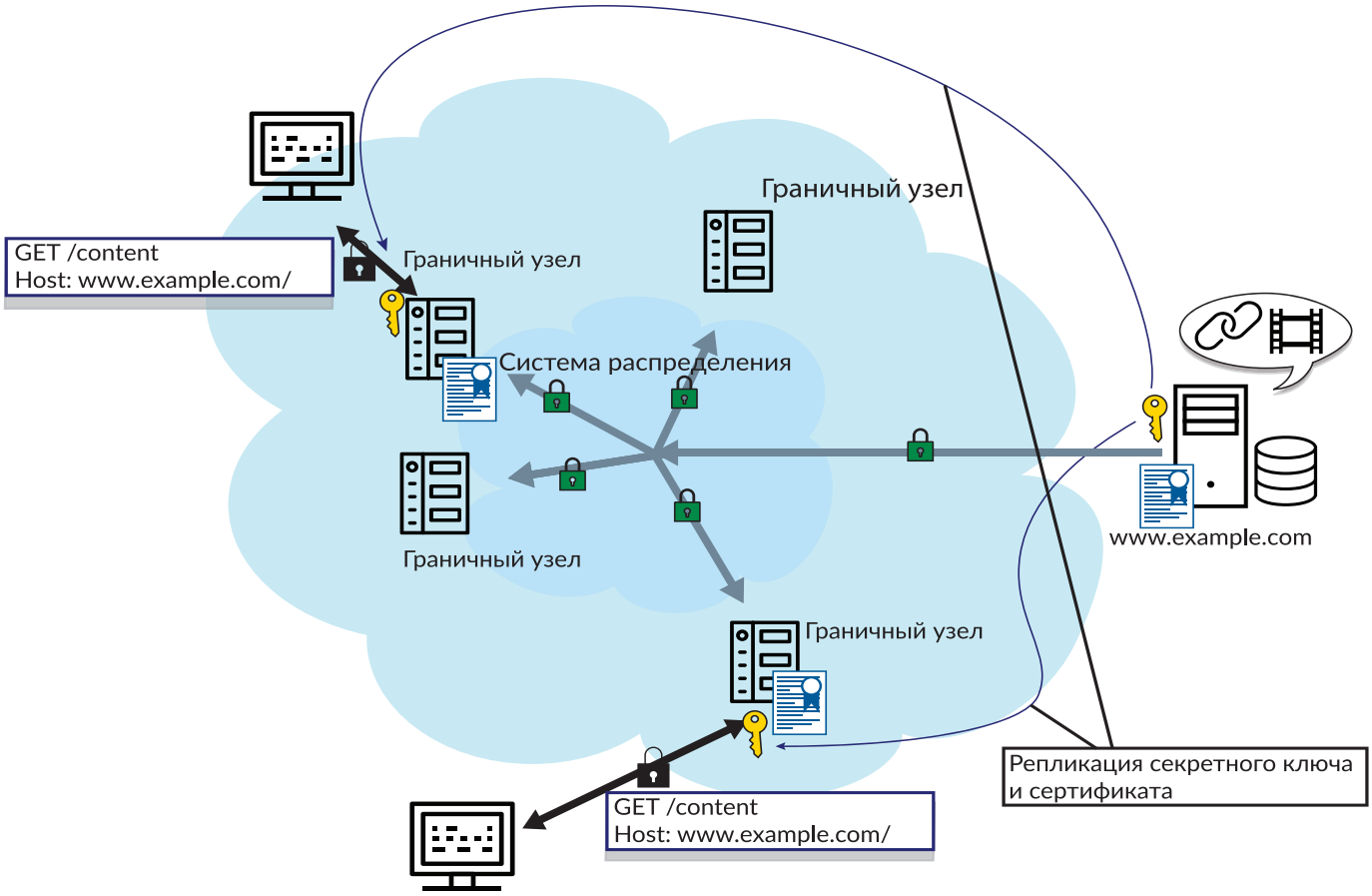


Рис. 4. Размещение TLS-сертификата и соответствующего секретного ключа на граничных узлах, обслуживающих зашифрованный контент.



ной детализации конкретного запрашиваемого объекта. Для этого используются методы маршрутизации на транспортном уровне и уровне приложений.

Маршрутизация запросов на транспортном уровне

При использовании этого механизма система маршрутизации анализирует информацию первого пакета запроса клиента на транспортном уровне. Обычно анализом пакета занимается граничный узел, который был выбран с использованием DNS. При этом система получает информацию о фактическом IP-адресе клиента и протоколе приложений, который этот запрос использует. Эта информация позволяет определить более оптимальный граничный узел и при необходимости перенаправить запрос.

Некоторые CDN используют гибридную схему, когда DNS транслирует имя в IP-адрес аникаст-узлов, которые отвечают за поиск оптимального граничного кэширующего узла и перенаправление запроса. Однако это перенаправление происходит незаметно для клиента. Трюк заключается в том, что аникаст-узел продолжает получать запросы от клиента, а ответы, собственно содержащие данные, передаются клиенту непосредственно с граничного узла. При этом граничный узел «выдает себя» за аникаст-узел, подменяя IP-адрес источника пакетов на аникаст-IP.

Маршрутизация запросов на уровне приложений

Анализ запроса на уровне приложений дополнительно позволяет получить информацию о запрашиваемом объекте (или объектах) контента и, соответственно, обеспечить наиболее оптимальную маршрутизацию.

Типичным является анализ запрашиваемого URL для более точного определения обслуживающего граничного узла или ближайших кэшей более высокого уровня, содержащих запрашиваемые данные.

Также часто используется анализ заголовков, таких как Cookie, Accept-language и User-agent, для определения более оптимального источника данных. Куки используются для идентификации клиента сайта или веб-сессии.

Для перенаправления запроса используется возможность протокола HTTP сигнализировать новый маршрут с помощью кода перенаправления (коды «302 Found» или «307 Temporary Redirect»). В этом случае ответ содержит новый URL, который приложение должно использовать для доступа к контенту.

Иногда маршрутизация запросов для встроенных объектов, например, изображений, может осуществляться в момент загрузки страницы. В этом случае используется техника «переписывания URL», когда встроенные директивы HTTP переписываются на лету, указывая на наиболее оптимальное для данного клиента расположение объектов.

Взаимодействие CDN

Архитектура Интернета основана на взаимодействии сетей. В Интернете отсутствует «ядро», или опорная сеть, напротив, глобальная связность обеспечивается путем взаимодействия множества независимых сетей, а не одним суперпровайдером. Логично предположить, что аналогичная модель будет работать и для доставки контента. Вместо того, чтобы расширять собственную сеть в зонах, где уже присутствуют CDN, сеть может осуществлять «делегиро-

вание» доставки другим CDN, тем самым объединяя ресурсы и увеличивая общую эффективность.

Решением данной проблемы, разработкой и стандартизацией соответствующих протоколов занимаются несколько организаций, включая ETSI (http://www.etsi.org/), Alliance for Telecommunications Industry Solutions (ATIS, http://www.atis.org/). Также разработка открытых интерфейсов взаимодействия ведется в рамках проекта EC Open ContEnt Aware Networks (OCEAN, http://cordis.europa.eu/project/rcn/94031_en.html). В этой статье я подробно расскажу о подходе, который был стандартизован в рамках рабочей группы CDNI IETF.

В этом случае возможным сценарием доставки контента может быть следующий процесс:

- Изначальный запрос от потребителя контента (пользователя) принимается авторитетной CDN – CDN, обслуживающей провайдера контента в рамках соответствующего соглашения. Часто такую CDN называют CDN вверх по потоку (Upstream CDN, uCDN).
- Авторитетная CDN может обслужить запрос самостоятельно или же перенаправить его другой CDN, в случае, если последняя может сделать это лучше (например, вследствие близости к пользователю). Такую CDN называю CDN вниз по потоку (Downstream CDN, dCDN).
- В ответ браузер пользователя запросит контент у dCDN, который, если требуется, будет подкачан из авторитетной uCDN и, если необходимо, от провайдера контента.

Другим примером, где такого рода взаимодействие CDN было бы полезно, является создание федераций. Многие крупные провайдеры широкополосного доступа внедряют собственные CDN. Однако поскольку зона обслуживания таких провайдеров часто включает различные регионы, соответственно, и CDN являются разобщенными. Обмен данными между ними путем создания «федеративной» CDN позволил бы решить эту проблему.

Общая модель взаимодействия между двумя CDN представлена на рис. 3. Как видно, обмен данными необходимо обеспечить между соответствующими подсистемами CDN, которые мы обсуждали ранее в этой статье.

Кратко остановимся на интерфейсах этого взаимодействия:

- CDNI Control interface (CI). Управляющий интерфейс, обеспечивающий обмен данными между системами управления CDN. Этот интерфейс необходим для инициализации всех остальных интерфейсов. В этом смысле он также иногда называется Trigger Interface.
- CDNI Logging interface (LI). Через этот интерфейс происходит обмен информацией об операциях CDN. Например, взаимодействующие CDN могут использовать этот интерфейс для мониторинга трафика в реальном времени, либо асинхронно обмениваться данными для анализа работы и финансовых расчетов.
- Интерфейс маршрутизации запросов отвечает за операции, необходимые для определения, какая CDN (и, возможно, какой граничный сервер) будет обслуживать запрос пользователя. Этот интерфейс состоит из двух взаимосвязанных интерфейсов:

Рис. 5. Предлагаемая структура распределения ключей и доступа к ним в рамках модели LURK.

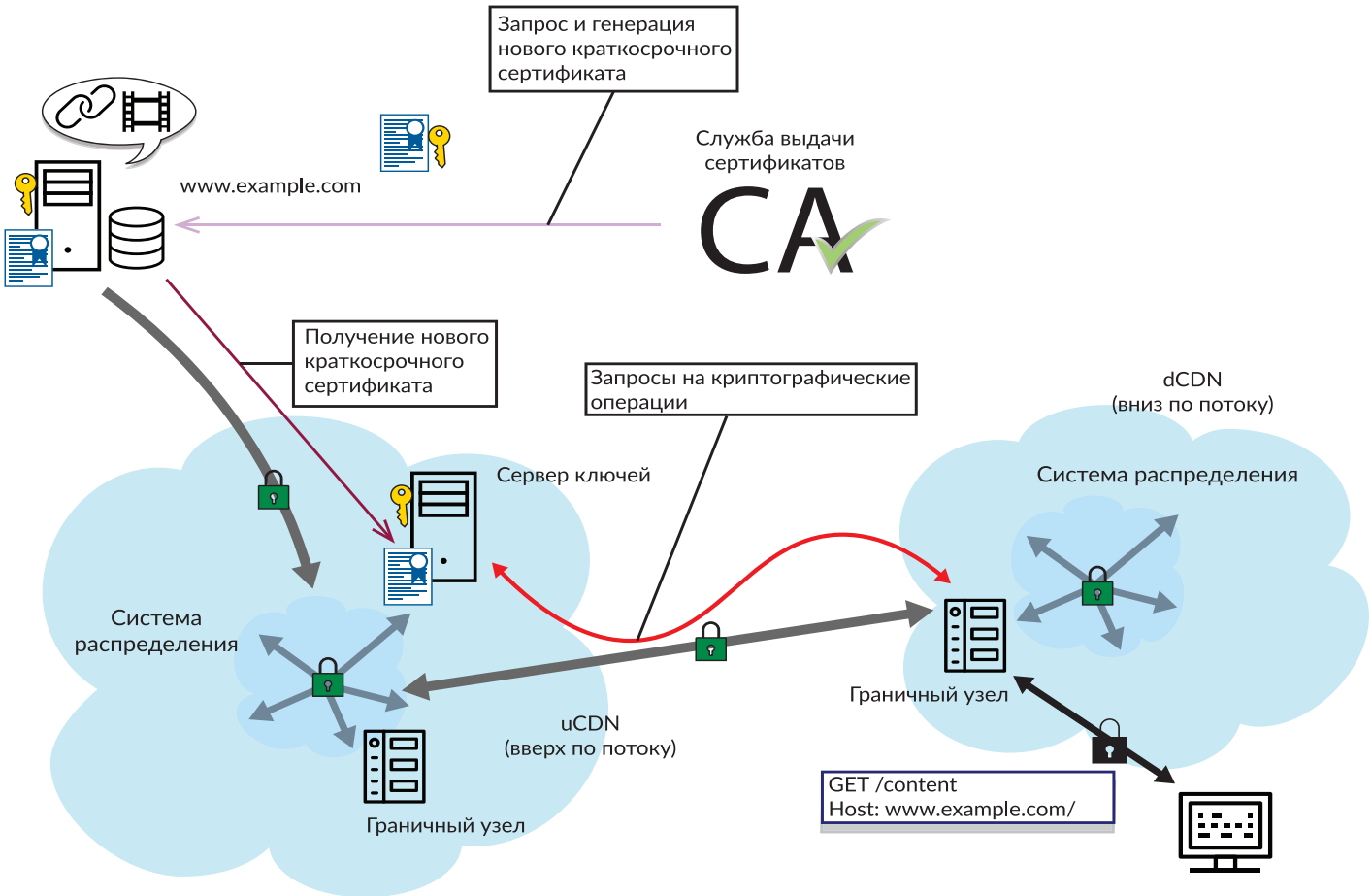
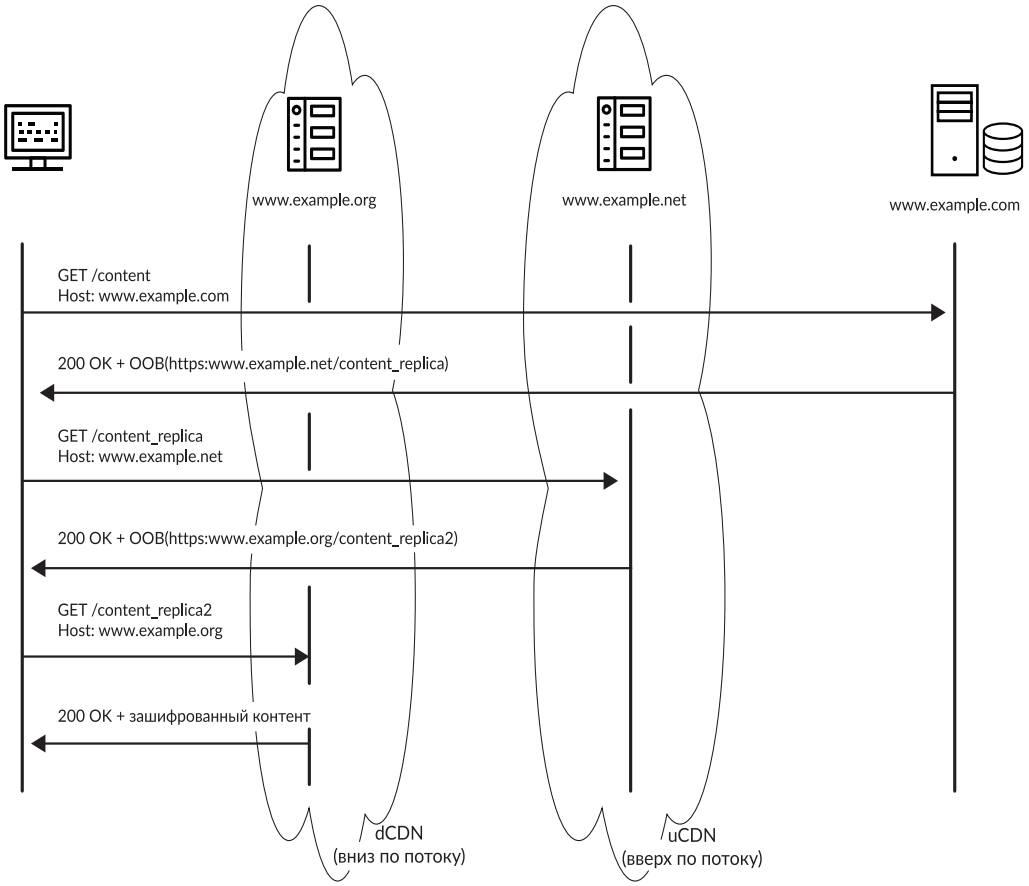


Рис. 6. Обмен запросами при использовании технологии OOB.



- CDNI Footprint & Capabilities Advertisement interface (FCI). Через этот интерфейс осуществляется асинхронный обмен информацией, требуемой для маршрутизации запросов, а именно информацией о зоне охвата и возможностях CDN.

- CDNI Request Routing Redirection interface (RI). Этот интерфейс обеспечивает синхронные операции для определения CDN, отвечающую за доставку контента пользователю в ответ на конкретный запрос.

- CDNI Metadata interface (MI). Этот интерфейс обеспечивает обмен метаданными, определяющими параметры обслуживания контента CDN. В качестве примера таких метаданных можно привести указания по геоблокированию, временные промежутки доступности контента и параметры доступа.

На сегодня основные спецификации, определяющие параметры этих интерфейсов и формат данных, стандартизованы. Приведу основные из них:

- RFC 8006 "CDN Interconnection Metadata" (https://datatracker.ietf.org/doc/rfc8006/)

Эта спецификация определяет формат метаданных и протокол для обмена. Метаданные, связанные с определенным контентом, предоставляют dCDN информацию, необходимую для обслуживания запросов пользователя.

- RFC 7975 "Request Routing Redirection interface for CDN Interconnection" (https://datatracker.ietf.org/doc/rfc7975/)

Этот документ определяет формат данных и протокол запросов uCDN другой о возможности последней обслужить конкретный пользовательский запрос. Также он определяет ответ обслуживающей dCDN, содержащий информацию о параметрах перенаправления пользовательского запроса.

- RFC 7937 "CDNI Logging Interface" (https://datatracker.ietf.org/doc/rfc7937/)

Эта спецификация определяет структуру и протокол обмена информацией об операциях между взаимосвязанными CDN, а также формат файлов регистрационного журнала.

- RFC 8007 "CDNI Control Interface / Triggers" (https://datatracker.ietf.org/doc/rfc8007/)

Эта спецификация определяет часть интерфейса CI, позволяющего одной CDN вызвать определенные действия со стороны другой CDN, которой делегирована доставка контента пользователю. Примером таких действий может быть подготовка контента и метаданных или очистка метаданных и кэша.

- RFC 8008 "CDNI Request Routing: Footprint and Capabilities Semantics" (https://datatracker.ietf.org/doc/rfc8008/)

Этот документ определяет требования к протоколу FCI и, в частности, тип и формат данных, необходимых для извещения других CDN (выше по потоку) о возможностях и зоне охвата данной CDN.

- URI Signing for CDN Interconnection (https://datatracker.ietf.org/doc/draft-ietf-cdni-uri-signing/). Эта спецификация находится в заключительной стадии стандартизации.

Этот документ описывает, как концепция электронной подписи URI обеспечивает контроль доступа, и предлагает метод подписи URI.

Обеспечение защищенных соединений при взаимодействии CDN

Использование протокола TLS/HTTPS для шифрования данных и аутентификации веб-серверов становится все более общей практикой. При этом весь трафик между браузером и сервером зашифрован на уровне приложений, означая, что все данные HTTP, включая заголовки, URL и собственно сам контент, являются недоступными для промежуточных устройств.

Это, безусловно, представляет проблему для CDN. Отсутствие доступа к этим данным означает, что контент невозможно кэшировать, не представляется возможным манипулировать с заголовками и проводить анализ трафика для оптимальной маршрутизации запросов. Означает ли это, что сайты, использующие HTTPS, не могут эффективно обслуживаться CDN?

Для решения этой проблемы граничные

узлы и система мониторинга должны иметь доступ к незашифрованному контенту. Обычно это достигается путем размещения секретного ключа и сертификата TLS, объединяющего параметры ресурса (полное доменное имя и организацию-оператор) с соответствующим публичным ключом, на каждом граничном узле, обслуживающем этот контент. Этот процесс схематично показан на рис. 4. В этом случае каждый граничный узел может расшифровать передаваемые данные и вновь зашифровать его для передачи от и к поставщику контента (веб-сайту) по внутренней сети CDN. Для этого могут использоваться другие ключи и схемы шифрования.

Однако этот подход несет в себе существенные риски. Хранение секретного ключа в десятках, если не в сотнях тысяч узлов, каждый из которых может иметь уязвимые места, открывающие возможность несанкционированного доступа, представляет серьезную опасность и накладывает серьезные требования на защищенность узлов CDN. Добавим, что каждый граничный узел хранит не один, а множество секретных ключей сайтов, которые данная CDN обслуживает.

Для решения этой проблемы рассматриваются несколько подходов.

LURK

В рамках совещания IETF96 в июле 2016 года был организован BoF LURK (Limited Use of Remote Keys, Ограниченное использование удаленных ключей) для обсуждения решения этой проблемы. Суть предлагаемой архитектуры заключается в следующем:

Вместо размещения секретного ключа на граничном узле предлагается использовать сервер ключей для удаленного выполнения криптографических операций. Авторизованные граничные узлы обращаются к серверу ключей для выполнения криптографических операций, в частности, для генерирования симметричного секретного сеансового ключа, используемого для шифрования данных. Даже если один из граничных узлов является скомпрометированным, это повлияет только на запросы, обслуживаемые этим узлом, а не на всю систему в целом, как в случае неавторизованного доступа к секретному ключу. Такой же подход может применяться для взаимодействующих CDN в рамках модели CDNI, которую мы только что рассмотрели. В этом случае CDN, которой делегирована функция доставки контента пользователю, должна получить доступ к серверу ключей.

Модель такой архитектуры представлена на рис. 5.

Внеполосное перенаправление (Out-of-band, OOB)

Этот подход, детально описанный в проекте спецификации «'Out-Of-Band' Content Coding for HTTP» (https://datatracker.ietf.org/doc/html/draft-reschke-http-oob-encoding), предлагает использование нового заголовка accept-encoding для указания местонахождения реплики запрашиваемого контента.

Работает это следующим образом: клиент (веб-браузер) отправляет первичный запрос на сервер, обслуживающий контент, www.example.com. В ответ сервер посылает код 200 OK вместе с картой альтернативных мест получения этого контента. Браузер обращается к одному из новых серверов и получает контент.

Этот механизм перенаправления предназначен для использования в CDN, а в случае взаимодействующих CDN – CDNI. Преимуществом является то, что альтернативные реплики ресурсов адресуются собственными URL. Соответственно, и TLS-сертификаты находятся под их полным контролем и не нуждаются в делегировании или репликации.

Обмен запросами в случае взаимодействующих CDN показан на рис. 6.

Краткосрочные сертификаты

В идеале, в рамках подхода LURK владелец контента/веб-сайта должен контролировать и обслуживать сервер ключей. Однако это не является практически реализуемым по нескольким причинам. Во-первых, это усложнит инфраструктуру владельца контента, а упрощение инфраструктуры является одним из мотивирующих факторов использования услуг CDN. Во-вторых, необходимость обслуживания запросов на криптографические операции с каждого граничного узла будет иметь серьезные негативные последствия для производительности и устойчивости всей системы. По этим причинам оператор CDN скорее всего создаст собственную масштабируемую инфраструктуру серверов ключей. Это оставляет проблему размещения секретного ключа в инфраструктуре оператора CDN нерешенной.

Использование краткосрочных (например, сроком действия три дня) сертификатов может уменьшить серьезность этой проблемы. В этом случае CDN периодически запрашивает у владельца контента новый сертификат и связанную с ним пару ключей (секретный и публичный). Владелец контента должен иметь возможность получения сертификата с помощью автоматизированного процесса, например, ACME (https://datatracker.ietf.org/wg/acme/documents/). Разумеется, обмен данными происходит в зашифрованном виде.

Другая идея заключается в использовании так называемых делегированных сертификатов (https://datatracker.ietf.org/doc/html/draft-rescorla-tls-subcerts). Суть ее заключается в создании ограниченного механизма делегирования, который позволяет оператору сервера TLS выдавать свои учетные данные в рамках сертификата, выданного внешним центром сертификации. Поскольку такое делегирование, осуществляемое путем создания подчиненного сертификата, не связано с функцией CA по проверке владения именами, оно является безопасным, если получатель делегации выступает только от имени, разрешенного родительским сертификатом.

В настоящее время LURK, Внеполосное перенаправление и краткосрочные и делегированные сертификаты находятся на ранней стадии разработки. Однако некоторые прототипы уже существуют для OOB и LURK. Время покажет, насколько широким станет их внедрение. Станут ли основой архитектуры CDN стандарты CDNI или будущее останется за более закрытыми подходами, такими как расширение CDN с использованием облачной инфраструктуры, или решений типа OpenPlay (http://www.jet-stream.com/blog/open-play-the-background/).

Общий регламент ЕС по защите персональных данных

Джейн Финлейсон-Браун (Jane Finlayson-Brown),
Ванне Пеммелаар (Wanne Pemmelaar)

После четырех с лишним лет обсуждения новая рамочная система защиты персональных данных в ЕС была принята 8 апреля 2016 года в форме регламента – Общего регламента по защите персональных данных, General Data Protection Regulation (GDPR)[1]. GDPR заменит действующую Директиву о защите персональных данных и будет непосредственно применяться во всех странах-участницах Евросоюза без необходимости в разработке имплементирующего национального законодательства. Регламент будет введен в действие 25 мая 2018 года. Вместе с тем, Регламент будет иметь немедленный эффект, поскольку он содержит ряд весьма обременительных для организаций обязательств, реализация которых потребует времени.

Данное законодательство привлекло массу внимания уже начиная с 2012 года, когда соответствующая законодательная инициатива впервые была вынесена Еврокомиссией на обсуждение. Законопроект даже влиял на решения, принимаемые Судом Евросоюза. Организации во всех странах ЕС и за его пределами испытывали все большие неудобства из-за прогрессирующей дисгармонии между законами стран-участниц Евросоюза по защите персональных данных, несмотря на растущие потоки данных через границы. GDPR хотели принять как можно быстрее, даже если это означало бы, что урегулирование некоторых деталей пришлось бы отложить на потом. И законодатели Евросоюза не стали тянуть время. Принятие GDPR знаменует собой новую веху в законодательстве ЕС о защите персональных данных.

Чтобы помочь организациям подготовиться к новому законодательству, Рабочая группа Статьи 29 (WP29), состоящая из представителей органов по защите данных (далее Data Protection Authorities, DPA) стран-участниц ЕС, разрабатывает разъяснения по различным аспектам GDPR. Первые разъяснения об инспекторах защиты данных, принципе единого окна и новом праве портативности персональных данных были приняты 5 апреля 2017 года, и в течение 2017 года выйдет еще ряд разъяснений.

В настоящей статье мы осветим ряд значимых моментов GDPR.

Что вам необходимо знать

РАСШИРЕНИЕ ТЕРРИТОРИАЛЬНОЙ ЮРИСДИКЦИИ

GDPR распространяется на организации[2] за пределами ЕС, , чья деятельность по обработке персональных данных связана с предложением товаров и услуг (даже безвозмездным) субъектам данных в ЕС или с мониторингом их поведения на территории ЕС. Многим таким организациям потребуется назначить представителя в ЕС.

«Теперь, с принятием GDPR, будущее защиты персональных данных в ЕС прояснилось и началась подготовка к внедрению нового регламента».

Дэвид Смит (David Smith),
специальный консультант Allen & Overy

«...Значительный шаг по направлению к Единому цифровому рынку».

Андрус Ансип (Andrus Ansip),
вице-президент Европейской Комиссии по Единому цифровому рынку

«Расширение территориального охвата GDPR обеспечит более сбалансированное взаимодействие между контролерами данных в ЕС и за его пределами».

Найджел Паркер (Nigel Parker)
– партнер, Allen & Overy

В преамбуле содержится ряд полезных разъяснений. «Предложение товаров и услуг» – это больше, чем просто доступ к веб-сайту или адресу электронной почты. Свидетельством такого предложения может быть использование языка или валюты, традиционно используемых в одной или нескольких странах-участницах ЕС, при наличии возможности заказывать товары/услуги в этой стране или странах и/или осуществлять мониторинг клиентов или пользователей на территории ЕС. «Мониторинг поведения» происходит, к примеру, при отслеживании поведения пользователей в Интернете с помощью методов, позволяющих профилирование пользователя с целью принятия решений о нем или прогнозирования его личных предпочтений и т.п.

На практике это означает, что компания за пределами ЕС, ориентированная на потребителей в странах ЕС, в будущем подпадет под действие GDPR. Сейчас это не так.

ОТЧЕТНОСТЬ И КОНСТРУКЦИОННО ЗАЛОЖЕННАЯ КОНФИДЕНЦИАЛЬНОСТЬ

GDPR налагает на контролеров данных очень обременительные обязанности.

В частности, они обязаны:

- вести определенную документацию,
- выполнять оценку воздействия обработки персональных данных на права субъектов данных для более рискованных видов обработки (составление списков таких видов операций возлагается на DPA),
- внедрить защиту данных на конструкционном уровне и по умолчанию, например, используя подход минимизации данных.

ИНСПЕКТОРЫ ПО ЗАЩИТЕ ДАННЫХ

В определенных обстоятельствах обработчики и контролеры данных будут обязаны назначить инспектора по защите данных (Data Protection Officer, DPO) в рамках своей программы отчетности. Назначение инспектора обязательно в следующих случаях:

- обработка данных осуществляется госорганом,
- основная деятельность контролера или обработчика заключается в такой обработке, которая по своей сути, масштабу или целям требует крупномасштабного, регулярного и систематического мониторинга субъектов данных, или
- основная деятельность организации заключается в крупномасштабной обработке специальных категорий данных.

DPO должен обладать достаточной экспертной квалификацией, определяемой характером операций по обработке данных, за которые инспектор будет отвечать.

DPO может быть сотрудником организации или работать с ней по сервисному контракту. Группа организаций или определенные группы государственных учреждений могут назначить одного DPO (при условии его доступности для всех участников). Руководящие положения WP29, опубликованные в апреле 2017 года, разъясняют некоторые аспекты GDPR в отношении DPO, включая то, что DPO в принципе должен находиться на территории ЕС и быть непосредственно подчинен высшему уровню руководства организации.

РОЛЬ ОБРАБОТЧИКОВ ДАННЫХ

Одним из важнейших нововведений GDPR является то, что у обработчиков данных впервые появились прямые обязанности. Сюда относятся следующие обязанности: вести письменный реестр операций по обработке персональных данных, выполненных от имени и по поручению каждого контролера; назначить, если требуется, инспектора по защите данных; назначить при определенных обстоятельствах представителя в ЕС (если у обработчика нет представительства в ЕС); уведомлять контролера об обнаруженных утечках персональных данных без необоснованной задержки. Положения о трансграничной передаче данных также распространяются на обработчиков, включая теперь формально признанные для обработчиков данных «Обязательные корпоративные правила» (Binding Corporate Rules, BCR).

Новый правовой статус обработчиков данных наверняка повлияет на то, как вопросы защиты данных будут отражаться в договорах поставки и других коммерческих соглашениях.

«Многие компании уже сейчас пересматривают свои процессы и процедуры, чтобы обеспечить соблюдение GDPR».

Найджел Паркер (Nigel Parker)
– партнер, Allen & Overy

СОГЛАСИЕ СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ НА ОБРАБОТКУ

Согласие должно быть дано свободно, быть конкретным, информированным и однозначным. Запросы на получение согласия должны быть отделены от других условий, а также изложены четким и понятным языком.

Согласие на обработку персональных данных должно быть настолько же легко отозвать, как и предоставить. Для специальных категорий данных согласие должно быть явно выраженным. Контролер данных обязан быть в состоянии предоставить доказательства получения согласия. Согласие, полученное в соответствии с текущим законодательством, может считаться действительным при условии, что оно отвечает новым требованиям.

Продолжается дискуссия о том, является ли согласие допустимым правовым основанием для обработки данных в случаях, когда между субъектом данных и контролером данных существует значительное неравенство. GDPR утверждает, что при оценке добровольности согласия необходимо учитывать, в частности, то, поставлено ли исполнение договора в зависимость от предоставления согласия субъектом на обработку его данных, которые для исполнения этого договора не нужны. Данное требование может, в частности, повлиять на предоставление услуг электронной коммерции. Кроме того, страны-участницы ЕС вправе устанавливать дополнительные требования к использованию согласия в контексте трудовых отношений. Преамбула разъясняет, что согласие не считается добровольным, если субъект данных не имеет подлинного и свободного выбора либо возможности отказать в предоставлении согласия или отозвать согласие без ущерба для себя.

При обработке персональных данных в целях прямого маркетинга субъект данных имеет право заявить возражение против обработки, и субъекта необходимо недвусмысленно поставить в известность о наличии такого права.

Другой темой, вызвавшей жаркие споры, стали требования к согласию родителей на оказание детям услуг информационного общества. Достигнутый компромисс (страны-участницы смогут снизить возраст ребенка, когда согласие родителей не требуется, с 16 до 13 лет) приведет к возникновению разнобоя в применимых требованиях, и компании, работающие сразу в нескольких странах Евросоюза, скорее всего выберут самый высокий из стандартов. Однако в преамбуле сказано, что согласие родителей не требуется для оказания превентивных или консультационных услуг, предлагаемых непосредственно ребенку.

ИНФОРМАЦИЯ О ДОБРОСОВЕСТНОЙ ОБРАБОТКЕ ДАННЫХ

Контролеры данных по-прежнему обязаны предоставлять субъектам данных прозрачную информацию об обработке, причем в момент сбора персональных данных. Существующие формы уведомлений об обработке должны быть пересмотрены, поскольку требования GDPR гораздо более детализированы по сравнению с действующей Директивой. Например, по новым правилам уведомление должно содержать более обширную информацию, а также ставить субъекта данных в известность о его правах (таких как право на отзыв согласия) и о сроке хранения данных.

Контролерам потребуется привести свои формы уведомлений в соответствие с новыми требованиями и представить информацию понятно и в легкодоступном формате.

УВЕДОМЛЕНИЯ ОБ УТЕЧКАХ ДАННЫХ

Контролеры данных обязаны сообщать DPA о большинстве утечек данных, без неоправданной задержки – по возможности в течение 72 часов после обнаружения утечки. При несоблюдении этого срока требуется предоставить мотивированное обоснование. В некоторых случаях контролер данных также обязан без неоправданной задержки уведомить об утечке субъектов данных.

Руководящие положения WP29 по уведомлениям об утечках данных ожидаются во второй половине 2017 года.

На первый взгляд, эта норма обременительна и для контролеров данных, и для DPA. Однако в ряде отраслей организации уже обязаны сообщать об утечках данных. Например, британское Управление по защите данных (UK ICO, Information Commissioner's Office, прим. ред.) уже требует организации уведомлять обо всех «серьезных» утечках.

Регламент также содержит пороговый уровень: уведомлять DPA не обязательно, если вероятность возникновения риска для прав и свобод граждан в результате утечки данных невелика. Пороговым уровнем для уведомления субъектов данных является наличие «высокого риска» для их прав и свобод. Хотя пороговые уровни смягчат нагрузку на организации, связанную с введением этого обязательства, все компании будут в любом случае обязаны внедрить внутренние процедуры реагирования на инциденты с персональными данными.

ШТРАФЫ

GDPR устанавливает многоуровневые санкции за нарушения законодательства о защите данных, позволяющие DPA назначать штрафы за некоторые нарушения в размере, достигающем наибольшей из двух цифр: 4% годового мирового оборота организации или 20 миллионов евро (в частности, за нарушение требований к международной передаче данных или основных принципов обработки, таких как условия для получения согласия). Другие нарушения могут повлечь за собой штраф в размере 2% годового мирового оборота или 10 миллионов евро (опять же берется большая из двух цифр). Текст включает список обстоятельств, принимаемых во внимание при определении размера штрафа (таких как характер, тяжесть и продолжительность нарушения).

Процентный штраф налагается на «предприятия» («undertakings»), причем в преамбулу в последний момент было добавлено разъяснение, что термин «предприятие» трактуется в соответствии с положениями статей 101 и 102 Договора о функционировании Европейского Союза.

Высокие штрафы уже безусловно привлекают внимание высшего руководства организаций.

ПРИНЦИП ЕДИНОГО ОКНА

Механизм единого окна является одним из ключевых элементов GDPR. Ожидалось, что он позволит компаниям, действующим сразу в нескольких странах ЕС, подпадать под надзор только одного "ведущего DPA". Однако на деле механизм оказался гораздо сложнее, так как проводит различие между внутринациональной и трансграничной обработкой данных.

Для ситуаций, подпадающих под принцип единого окна, вводятся сложные процедуры по координации и сотрудничеству между национальными DPA.

Чтобы позволить частным лицам обращаться за решением дел локально, GDPR содержит подробную систему сотрудничества между так называемым ведущим DPA и другими "компетентными DPA", которая позволяет адекватно разрешать местные и срочные дела. WP29 опубликовала разъяснения о том, как определить ведущее DPA. Как принцип одного окна будет работать на практике и не приведет ли он к практике поиска удобной юрисдикции, пока неизвестно.

ОТМЕНА УВЕДОМЛЕНИЙ DPA

Приятным изменением для контролеров данных стала отмена обязанности уведомлять DPA об обработке данных или получать разрешения DPA. Цель этого изменения - снизить административную и финансовую нагрузку на контролеров данных, хотя в результате DPA некоторых стран будут вынуждены искать новые источники финансирования.

Вместо обязанности уведомлять DPA контролеры данных теперь несут ответственность за операции по обработке персональных данных. Например, контролеры данных обязаны внедрить эффективные процедуры и механизмы для более рискованных операций с данными (например, с использованием новых технологий) и провести оценку последствий обработки для защиты персональных данных ("data protection impact assessment", PIA), чтобы определить вероятность и тяжесть рисков, особенно при крупномасштабной обработке. Усилия, которые для этого потребуются, и потенциальные штрафы за несоблюдение скорее всего перевесят преимущества, предоставленные уменьшением административной нагрузки в связи с отменой уведомлений. Кроме того, вводится новое требование заблаговременно обращаться в DPA за консультацией в случае, если PIA выявит наличие высоких рисков для безопасности данных при их обработке в отсутствие мер по снижению этих рисков. Если по мнению DPA обработка приведет к нарушению GDPR, DPA может предоставить письменные рекомендации, а при необходимости и использовать правоприменительные полномочия. Требование о консультации с DPA создает неопределенность для контролеров, так как они должны будут оценить результаты

PIA и принять решение, обращаться ли за консультацией.

НОВЫЙ ЕВРОПЕЙСКИЙ СОВЕТ ПО ЗАЩИТЕ ДАННЫХ

Независимый Европейский совет по защите данных (European Data Protection Board, EDPB) заменит WP29. Он будет состоять из руководителя Европейской службы по защите данных и старших представителей национальных DPA Евросоюза. Роль Совета заключается в публикации заключений и руководящих положений, обеспечении единообразного применения GDPR и отчетности перед Еврокомиссией. Также Совет играет ключевую роль в механизме единого окна.

ОБЯЗАТЕЛЬНЫЕ КОРПОРАТИВНЫЕ ПРАВИЛА (BCR)

GDPR прямо признает обязательные корпоративные правила ("binding corporate rules", BCR) для контролеров и обработчиков как способ для законной трансграничной передачи данных в рамках одной корпоративной группы. BCR должны быть юридически обязательны для всех членов группы, осуществляющих совместную экономическую деятельность, распространяться на всех членов группы и применяться каждым членом группы, включая их сотрудников. BCR должны непосредственно наделять субъектов данных юридически закрепленными правами. Положения GDPR включают четкий перечень требований к BCR.

Многие считают BCR «золотым стандартом», и в дальнейшем они, вероятно, приобретут все большую популярность для передачи данных в рамках корпоративной группы.

МЕЖДУНАРОДНАЯ ПЕРЕДАЧА ДАННЫХ

Тех, кто надеялся на полный пересмотр этой области, ждет разочарование, поскольку GDPR содержит практически тот же самый инструментарий. Трансграничная передача данных будет облегчена благодаря отмене требований по предварительному одобрению DPA операций по передаче данных, основанных на признанных механизмах по обеспечению адекватной защиты прав субъектов данных, например, типовых контрактах, одобренных Еврокомиссией или DPA. С другой стороны, GDPR отменит такое удобное основание для передачи данных как самостоятельная оценка организацией, ныне используемое как отдельное основание для передачи данных только в нескольких странах Евросоюза и которым, очевидно, пожертвовали в целях унификации.

Также дополнены положения о согласи субъекта: экспортеры данных, полагающиеся на согласие для передачи данных за пределы ЕС, должны будут внимательно следить за тем, чтобы субъекты данных были надлежащим образом поставлены в известность о рисках такой передачи.

В качестве новой дерогации добавлена концепция законных интересов, но сфера ее применения невелика. Она может использоваться там, где международная передача является разовой, касается только нескольких субъектов данных, необходима для осуществления веских законных интересов (не перекрытых правами субъекта данных) и только если контролер оценил все обстоятельства и применил необходимые меры защиты. Также при этом требуется проинформировать DPA. Трудно представить себе практическую пользу этой дерогации. К облегчению многих, полный запрет на передачу данных иностранным госорганам без разрешения DPA не дожил до окончательной редакции.

ПРАВА СУБЪЕКТОВ ДАННЫХ

Одной из главных целей Европейской Комиссии при разработке новой рамочной системы защиты данных было повышение защиты прав граждан. Этот мотив четко прослеживается в усилении прав субъектов данных. В частности, это право лица требовать информации об обработке его персональных данных, право доступа к данным при определенных обстоятельствах и право исправления неправильных данных. Также имеется право ограничить определенную обработку и право возражать против обработки своих персональных данных для целей прямого маркетинга.

Граждане могут также потребовать возврата своих персональных данных в структурированном виде и распространенном формате для облегчения их передачи другому контролеру (так называемая портативность данных). В недавней инструкции WP29 разъяснено, как следует толковать и реализовать это право. Инструкция указывает, что контролеры данных, передающие обработку данных на аутсорсинг или осуществляющие ее совместно с другими контролерами, должны четко оговорить в контрактах обязанности каждой из сторон при реагировании на запросы лиц о переносе их данных, а также обязаны внедрить соответствующие процедуры.

Огромную известность, особенно после решения Европейского суда по иску Google против Испании, стало так называемое право на забвение, или право на удаление данных. В определенных ситуациях, таких как отзыв согласия, при отсутствии других законных оснований для обработки, субъект данных может потребовать от контролера немедленно удалить свои персональные данные. Также предусмотрена обязанность принять разумные меры к информированию третьих сторон о том, что субъект данных потребовал удаления любых ссылок на такие данные и любых их копий. На практике это будет часто трудноосуществимо.

Отметим, что контролер данных обязан реагировать на такие информационные запросы в течение месяца, с возможностью продлить этот срок для особо сложных запросов. Контролерам данных потребуется внедрить четкие процедуры для выполнения этих обязательств.

Информация должна предоставляться бесплатно, за исключением случаев, когда запрос является «явно необоснованным или чрезмерным».

Что дальше?

Регламент 2016/679 вступил в силу 25 мая 2016 года и будет введен в действие 25 мая 2018 года. С этого момента текущая Директива 95/46/ЕС потеряет силу. Сейчас, когда компании начали процесс перехода к новым требованиям, страны Евросоюза оценивают влияние регламента на национальное законодательство о защите данных.

«Уровень риска, связанный с GDPR, поставил вопросы защиты данных на повестку советов директоров».

Джейн Финлесон-Браун (Jane Finlayson-Brown)
– партнер, Allen & Overy

Хотя GDPR будет непосредственно применяться в странах-участницах Евросоюза, национальные законы потребуется модифицировать для урегулирования таких аспектов, как позиция DPA, отраслевые положения, переходные нормы, или для принятия дополнительных положений в ситуациях, предусмотренных GDPR.

Первые национальные законопроекты уже опубликованы, например, в Германии, Нидерландах и Польше.

МНОГИЕ КОМПАНИИ СЕЙЧАС ЗАДАЮТСЯ СЛЕДУЮЩИМИ ВОПРОСАМИ:

Какие новые обязанности по GDPR применимы к их организации?

Каковы различия между существующими требованиями и новыми стандартами?

Какие изменения нужно осуществить для выполнения требований GDPR, в какой срок, в каком порядке и с какими затратами?

Восемь шагов по подготовке

1. Подготовьтесь к утечкам данных

Внедрите четкие политики и отработанные процедуры для обеспечения того, чтобы вы могли быстро отреагировать на любую утечку данных и при необходимости своевременно оповестить о ней.

2. Создайте систему отчетности

Если требуется назначить инспектора по защите данных, сделайте это. Разработайте четкие документы, определяющие политику организации в отношении обработки персональных данных и демонстрирующие соответствие требуемым стандартам. Создайте культуру мониторинга, пересмотра и оценки операций по обработке данных, направленную на минимизацию объема обработки и хранения данных и оснащенную защитными механизмами. Проверьте, что ваш персонал обучен и понимает свои обязанности. Также потребуется провести оценку рисков конфиденциальности с возможностью аудита, чтобы выявить все рискованные операции по обработке данных и принять меры к устранению конкретных проблем.

3. Внедрите защиту данных на конструкционном уровне

Конфиденциальность частной жизни должна быть заложена в любой новый продукт или операцию по обработке с самого начала. О ней необходимо думать сразу, чтобы обеспечить структурированную оценку и систематическую проверку. Внедрение конфиденциальности на конструкционном уровне поможет и продемонстрировать выполнение требований закона, и предоставит компании конкурентные преимущества.

4. Проанализируйте, на каких правовых основах вы используете персональные данные

Пересмотрите ваши операции по обработке данных. Полагаетесь ли вы, например, на согласие субъектов данных или же можете продемонстрировать наличие законного интереса в обработке данных, не перекрываемого интересами субъекта данных? Компании часто считают, что для обработки данных им необходимо согласие субъектов. Но согласие - лишь один из множества способов обеспечить законность обработки, причем не всегда лучший (поскольку согласие можно отозвать). Если вы полагаетесь на согласие субъектов данных, проверьте, адекватны ли ваши документы и формы на получение согласия и является ли согласие добровольным, конкретным и информированным. Бремя доказательств ляжет на вас.

5. Проверьте ваши уведомления о защите данных и политики конфиденциальности

GDPR требует, чтобы предоставляемая информация была изложена четко и простым языком. Ваши политики должны быть прозрачными и легкодоступными.

6. Помните о правах субъектов данных

Будьте готовы к тому, что субъекты данных станут пользоваться своими правами по GDPR, в том числе правом портативности данных и правом на забвение. Если вы храните персональные данные, проверьте законность оснований для их хранения – именно на вас ложится бремя доказательства того, что ваши законные основания перекрывают интересы субъектов данных. Также будьте готовы к встрече с гражданами, имеющими крайне завышенное представление о своих правах.

7. Если вы поставщик, проверьте, не появились ли у вас новые обязанности обработчика

GDPR налагает на обработчиков прямые обязанности, которые вы должны понять и учесть в своих политиках, процедурах и контрактах. Также вероятно, что ваши заказчики потребуют от ваших услуг соответствия ужесточенным требованиям нового Регламента. Проверьте, адекватна ли ваша договорная документация, а для действующих контрактов – кто несет расходы по внесению необходимых изменений в оказание услуг в связи с изменением законодательства. Если услуги по обработке данных вам оказывает третья сторона, очень важно определить и документально закрепить обязанности сторон.

8. Трансграничная передача данных

При любой международной передаче данных, в том числе в рамках корпоративной группы, важно иметь законные основания для передачи персональных данных в юрисдикции, не обеспечивающие адекватный уровень защиты данных. Эта проблема не нова, но теперь, когда вам грозит штраф в размере 4% годового мирового оборота или 20 миллионов евро, последствия несоблюдения требований закона могут быть очень серьезными. Возможно, вам имеет смысл подумать о разработке обязательных корпоративных правил для облегчения передачи данных внутри группы.

[1] В контексте GDRP под защитой данных подразумевается защита персональных данных граждан. Далее в статье при использовании «защита данных» мы будем подразумевать защиту персональных данных (прим. ред.)

[2] Европейское законодательство по защите персональных данных определяет двух основных субъектов – «контролеров» и «обработчиков»:

«Контролер» означает физическое или юридическое лицо, официальный орган, агентство или иной орган, который самостоятельно или совместно с другими определяет цели и средства обработки персональных данных; в случае, когда цели или средства обработки определяются национальным законодательством или законами, или нормами Сообщества, контролер или особые критерии его назначения могут устанавливаться национальным законом или законом Сообщества.

«Обработчик» означает физическое или юридическое лицо, официальный орган, агентство или иной орган, который обрабатывает персональные данные по поручению контролера. (прим. ред.)

Источник: The EU General Data Protection Regulation, allenovery.com, (версия от 16.05.2017)

Контакты:

Антон Коннов, партнер, +7 495 725 7919

Игорь Горчаков, партнер, +7 495 662 6547

Jane Finlayson-Brown, +44 7767 674 407 (London office)
jane.finlayson-brown@allenovery.com

Wanne Pemmelaar, +31 622 796 799 (Amsterdam office)
wanne.pemmelaar@allenovery.com

Сбор и хранение данных пользователей: зарубежный опыт регулирования

Мадина Касенова

Интернет является центральным звеном телекоммуникаций, а история его применения приближается к пятидесятилетнему рубежу, при этом правовое регулирование использования Интернета едва ли насчитывает половину этого срока. Сложность правового регулирования отношений в сфере использования Интернета объясняется рядом факторов, ключевыми из которых являются, его трансграничный характер и специфический круг разнородных субъектов возникающих отношений.

Интернет является центральным звеном телекоммуникаций, а история его применения приближается к пятидесятилетнему рубежу, при этом правовое регулирование использования Интернета едва ли насчитывает половину этого срока. Сложность правового регулирования отношений в сфере использования Интернета объясняется рядом факторов, ключевыми из которых являются, во-первых, объективный характер многоуровневой технологической инфраструктуры Интернета, которая обеспечивает его трансграничное функционирование и использование; во-вторых, специфический круг субъектов возникающих отношений, охватывающий лиц различной юридической природы (субъектов публичного и частного права, субъектов, относящихся к различным правопорядкам).

В последнее десятилетие правовое регулирование использования Интернета в национальном праве расширяется и изменяется, затрагивая, в том числе, сферу отношений, связанных со сбором и хранением данных пользователей телекоммуникационных услуг. Вместе с тем, сохраняются различия подходов государств в формировании порядка, способов, форм и т.д. правового регулирования отношений, связанных с Интернетом, что во многом обусловлено политико-правовыми приоритетами государств, а также отражает разность подходов в понимании природы и сущностных свойств самого Интернета как сложного технологического и социального феномена.

Существующий плюрализм правового регулирования использования Интернета в национальном праве непосредственно выражается в закреплении ключевых и системообразующих понятий и терминов, определения их содержательных характеристик. Понятийно-категориальный аппарат правового регулирования формируется в конкретной правовой системе, а его использование имеет прикладное значение. К примеру, разграничение понятий «Интернет» (Internet) и «доступ к Интернету» (Internet access), их правовая квалификация существенным образом влияет на правовое регулирование использования Интернета, включая регулирование порядка сбора, использования, обработки и хранения данных пользователей Интернета, а также их защиту (далее – «Сбор данных пользователей») .

Представляется целесообразным обратиться в общем плане к правовому регулированию порядка сбора данных пользователей телекоммуникационных услуг в Федеративной Республике Бразилия и Соединенных Штатах Америки. Выбор этих государств обусловлен несколькими соображениями.

Федеративная Республика Бразилия стала первым государством, которое на уровне закона закрепило правовые основы, принципы и порядок использования Интернета, отразив фундаментальные технологические особенности многоуровневой инфраструктуры Интернета, обеспечивающие трансграничное функционирование и использование Интернета. Немаловажно, что в контексте существующих двусторонних отношений Россия-Бразилия, а также совместного участия этих государств в таком неформальном межгосударственном объединении, как БРИКС, обращение к опыту Бразилии представляется полезным.

США – государство, являющееся родиной Интернета, - относится к англо-американской правовой системе, отличающейся от континентальной правовой системы, к которой принадлежит большинство государств, включая Российскую Федерацию. В настоящее время в США регулирование порядка сбора данных пользователей телекоммуникационных услуг реформируется и диверсифицируется.

Федеративная Республика Бразилия 23 апреля 2014 года приняла законодательный акт – Закон № 12.965 «Marco Civil da Internet», далее – «Закон Marco Civil» , который исходит из самостоятельного значения понятий «Интернет» и «доступ к Интернету». При этом «доступ к Интернету» имеет первостепенное значение, является неотъемлемой частью осуществления прав и обязанностей граждан и гарантией комплекса прав пользователей, гарантированных ст. 7 Закона Marco Civil.

Следствием самостоятельного значения понятия «доступ к Интернету» является содержательное определение, в том числе таких понятий, как «интернет-соединение»,

«интернет-приложения», «запись о соединении/журнал соединений», «регистрация доступа к интернет-приложениям», а также функциональное разграничение «провайдеров интернет-соединений» и «провайдеров интернет-приложений», что в целом влияет на порядок регулирования отношений, связанных с использованием данных пользователей Интернета.

Согласно Закону Marco Civil, персональные данные, записи о соединениях и записи о доступе к интернет-приложениям, данные о частных интернет-коммуникациях пользователей носят конфиденциальный характер, а обязанность по их сохранности возлагается на интернет-провайдеров. Закон Marco Civil устанавливает, что сбор данных пользователей (включая персональные данные) может осуществляться в силу закона; может быть запрещен законом; может быть предусмотрен договором о предоставлении услуг или является условием использования интернет-приложений. В содержательном плане эти законодательные положения предполагают следующее.

1. Сбор данных пользователей осуществляется в силу действия нормативных положений Закона Marco Civil. Закреплены правовые основания сбора данных пользователей и обязанность ведения и хранения записей об интернет-соединениях пользователей, учетной документации о доступе при предоставлении соединения; учетной документации о доступе к интернет-приложениям (подразделы I, II, III, ст.ст. 13-15 Закона Marco Civil).

Для регулирования порядка сбора данных пользователей принципиально важным является законодательное закрепление и содержательное определение таких ключевых понятий, как «интернет-соединение», «запись о соединении/журнал соединений», «интернет-приложение», «регистрация доступа к интернет-приложению». Содержательно эти понятий означают:

«интернет-соединение» – наделение терминала способностью отправлять и получать пакеты данных по Интернету путем присвоения ему IP-адреса или его аутентификации;

«запись о соединении/журнал соединений» – массив информации, относящийся к дате и времени начала и завершения сессии подключения к Интернету, продолжительности такой сессии и использованию терминалом IP-адреса для отправки и получения пакетов данных;

«интернет-приложение» – набор функциональных средств, которые могут быть получены через подключенный к Интернету терминал; а также

«регистрация доступа к интернет-приложению» – «набор информации о дате и времени использования конкретного интернет-приложения, осуществляемого с конкретного IP-адреса».

Хранение и ведение записей об интернет-соединениях осуществляет организация, отвечающая за управление автономной системой и предоставляющая интернет-соединение (провайдер интернет-соединений). Ведение учета таких записей о соединениях не может быть передано третьим лицам. Провайдер интернет-соединений несет ответственность за хранение записей и обеспечивает их конфиденциальность; учет записей об интернет-соединениях хранится в течение 1 (одного) года, с соблюдением конфиденциальности, в контролируемом безопасном месте.

В качестве предупредительной меры административные и правоохранительные органы, а также Государственный прокурор могут потребовать хранить записи о соединениях в течение более длительного периода, т.е. больше года. При этом закреплена обязанность органа власти, потребовавшего предпринять такие предупредительные меры по хранению записей об интернет-соединениях, в течение 60 (шестьдесят) дней с момента первого запроса инициировать соответствующее судебное разбирательство. Во всех случаях провайдер интернет-соединений предоставляет регистрационные журналы, раскрывает иные данные исключительно на основании решения суда.

Хранение учетной документации о доступе к интернет-приложениям возлагается на провайдера интернет-приложений, который обязан вести журналы записей о предоставлении услуг доступа к приложениям, с соблюдением конфиденциальности, и хранить журналы в контролируемом и безопасном месте, в течение шести месяцев.

Если административные и правоохранительные органы, а также Государственный прокурор требуют хранить журналы записей о предоставлении услуг доступа к приложениям в течение более длительного периода, они обязаны в течение 60 (шестьдесят) дней с момента первого запроса инициировать соответствующее судебное разбирательство. Провайдер интернет-приложений раскрывает данные записей регистрационных журналов только на основании решения суда.

Провайдеры интернет-соединений и провайдеры интернет-приложений предоставляют информацию, подтверждающую, что сбор данных пользователей осуществляется в соответствии с действующим законодательством Бразилии о защите персональных данных и конфиденциальности данных пользователей.

2. Закон Marco Civil закрепляет гарантии прав пользователей, и такое законодательное закрепление гарантий прав обусловливает содержание функционирования органов власти.

Закон Marco Civil гарантирует соблюдение, в частности, следующих прав: право на неприкосновенность личной и частной жизни; право на неприкосновенность и конфиденциальность потоков интернет-коммуникации пользователей; право на невозможность приостановки интернет-соединения (кроме случаев задолженности); право на получение ясной и полной информации об обеспечении сохранности записей о соединениях и записей о доступе к интернет-приложениям в договорах об оказании услуг, а также о практике управления интернет-трафиком, которые могут повлиять на качество предоставляемых услуг; право на неразглашение третьим лицам персональных данных пользователя, включая записи о соединениях и записи о доступе к интернет-приложениям (за исключением случаев, когда пользователь выразил свое согласие добровольно и осознанно, либо в случаях, предусмотренных законом); право на полное исключение персональных данных по требованию пользователя, предоставленных им для использования данного интернет-приложения, при прекращении взаимоотношений сторон; право на открытость и прозрачность любых условий использования, устанавливаемых провайдерами интернет-соединений и провайдерами интернет-приложений и др. (ст. 7 Закона Marco Civil).

Законодательное закрепление гарантий прав, по сути, означает, что их ограничение запрещено, если иное не вытекает из решения суда и в порядке, установленном законом.

3. Закон Marco Civil устанавливает, что сбор данных пользователей может основываться и регулироваться соответствующими договорами о предоставлении услуг доступа или закрепляться в качестве условия использования интернет-приложений.

Законодательно гарантированному праву пользователей получать полную информацию о сборе, использовании, хранении, обработке и защите своих персональных данных (п. VIII ст. 7 Marco Civil) корреспондирует обязанность провайдеров закреплять в специальном пункте договора условие о сборе данных пользователя (п. IX ст. 7 Marco Civil). Договоры провайдеров интернет-соединений и провайдеров интернет-приложений, которые не соответствуют этим условиям, не имеют юридической силы в силу закона.

Важное значение имеют нормативные положения Закона Marco Civil, отражающие объективную трансграничную природу Интернета. Речь идет о том, что Закон Marco Civil специфицирует отношения и круг субъектов, к которым в императивном порядке применяется право Бразилии. Законодательно закреплено, что в императивном порядке право Бразилии применяется:

- в отношении любой деятельности по сбору, накоплению, хранению и обработке персональных данных или данных относительно интернет-соединений, если такая деятельность осуществляется в пределах государственной территории Бразилии;
- в отношении данных, собранных в пределах государственной территории Бразилии;
- к определению содержания интернет-контента, если по крайней мере один из терминалов расположен на территории Бразилии (под «терминалом» понимается компьютер или иное устройство, подключенное к Интернету);
- если деятельность по сбору, накоплению, сохранению и обработке персональных данных осуществляется юридическим лицом, расположенным за границей, но услуги оказываются неопределенному кругу лиц в Бразилии, или по крайней мере один из членов какой-либо хозяйствующей группы учрежден в Бразилии.

Соединенные Штаты Америки. В начале статьи отмечалось, что особенность правового регулирования в сфере использования Интернета определяется специфическим кругом субъектов регулируемых отношений, который охватывает субъектов различной юридической природы. В США провайдеры интернет-услуг – это компании частного сектора (субъекты частного права, созданные в соответствии с правом различных штатов США), соответственно, порядок, правила и процедуры, сроки и т.д. сбора данных пользователей относятся к «внутренней политике» компании (провайдера интернет-услуг) и регулируются внутренними регламентами и локальными актами таких компаний. Поскольку интернет-провайдеры являются компаниями частного сектора, они в «общеправовом плане» не обязаны раскрывать данные пользователей и вправе «проводить индивидуальную политику» по сбору данных пользователей.

С учетом особенностей правовой системы США, следует отметить, что в настоящее время в США сбор данных пользователей подпадает под регулирование законодательных актов федерального уровня и актов, принятых на уровне отдельных штатов. Актами федерального уровня являются, в частности, закон «О конфиденциальности электронных коммуникаций» (Electronic Communications Privacy Act, ECPA) 1986 г. (далее – «Закон ECPA») , действующий с изменениями, принятыми в 2015 году , закон «О конфиденциальности сообщений электронной почты (Email Privacy Act) 2016 г., разработанный в целях внесения поправок в Закон ECPA . На уровне штата принят закон «О конфиденциальности электронных коммуникаций штата Калифорния» 2015 г. (California Electronic Communications Privacy Act, CalECPA) .

К федеральному уровню относится закон «Об обмене и защите киберразведывательной информацией» (Cyber Intelligence Sharing and Protection Act, CISPA) , принятый при администрации прежнего президента США, который должен был вступить в силу в конце 2016 года (далее – «Закон CISPA»); а также закон «Об обмене информацией о кибербезопасности» (Cybersecurity Information Sharing Act, CISA) 2015 г. (далее – «Закон CISA») . До вступления в силу Закона CISPA Палата представителей Конгресса США проголосовала за его отмену, а одобрение Закона CISA администрацией нового президента США ожидается в ближайшее время.

Оговоримся, что предметом Закона CISPA и Закона CISA не является сбор данных пользователей, однако эти законы регулируют эту сферу отношений. Следует обратить внимание на кардинальную разницу в закреплении порядка регулирования сбора данных пользователей, предусмотренных названными законами. Закон CISPA предусматривал, что сбор данных пользователя (включая персональные данные, финансовые данные, данные о здоровье, детях, номера социальных страховок, записи о посещении веб-сайтов, информацию об использовании приложений, адреса электронной почты, содержание сообщений и проч.) и их использование осуществляется, во-первых, только на основании разрешения пользователя; во-вторых, пользователь вправе отказаться предоставлять такие данные. Новый Закон CISA закрепляет, что интернет-провайдеры вправе осуществлять сбор данных пользователей без их предварительного разрешения, а также предоставлять данные пользователей третьим лицам.

Тот факт, что Закон ECPA реформируется, Закон CISA еще не одобрен и окончательно не принят, а Закон CISPA отменен, дает основание сделать вывод о том, что в настоящее время в США на федеральном уровне нормативное регулирование в сфере сбора данных пользователей, закрепляющее соответствующие обязанности провайдеров интернет-услуг пользователей, формируется.

В США сбор данных пользователей осуществляется провайдерами интернет-услуг и, будучи компаниями частного сектора, интернет-провайдеры самостоятельно определяют порядок, правила, сроки сбора данных пользователей (хранения/удаления данных и проч.). Провайдеры интернет-услуг в том числе могут предусматривать условия сбора данных пользователей в договорно-правовом порядке: в пользовательских соглашениях компаний интернет-услуг, в договорах о предоставлении интернет-услуг и т.д. Провайдеры интернет-услуг так или иначе имеют доступ к данным пользователей, и даже если используется анонимный IP-адрес, провайдер интернет-услуг обладает возможностью идентифицировать его с IP-адресом пользователя, на котором зарегистрирована его учетная запись, соответственно, идентификация лица не представляет трудности для провайдера.

Вместе с тем провайдер интернет-услуг обязан осуществлять сбор данных пользователя по решению суда для представления этих данных правоохранительным органам. При этом сбор данных пользователя озна-

чает любые данные, включая персональные данные, информацию о кредитных картах, учетные записи о посещении веб-сайтов, информацию об этих веб-сайтах и т.д.

В ограниченных рамках статьи, тем не менее, следует отметить, что вопрос регулирования порядка сбора данных пользователей в США невозможно без упоминания происходящих процессов, связанных с инициативами по изменению правил защиты конфиденциальности данных, которые нуждаются в пояснениях следующего свойства.

В США Федеральная комиссия по связи США (Federal Communications Commission, FCC) обладает ключевыми полномочиями в принятии и реализации федеральной политики в регулировании отношений, связанных с использованием Интернета (далее – «Комиссия FCC»). Комиссия FCC 27 октября 2016 года одобрила «Правила конфиденциальности для пользователей широкополосного доступа, расширяющие возможности выбора прозрачности и безопасности [использования] их персональных данных» (Privacy Rules to Give Broadband Consumers Increased Choice, Transparency and Security for Their Personal Data). Согласно названному документу (далее – «Правила Privacy Rules»), в частности, предусматривалась обязанность интернет-провайдеров получать согласие пользователей на сбор их данных, вводились ограничения на предоставление интернет-провайдерами данных пользователей третьим лицам .

Правила Privacy Rules должны были вступить в силу в марте 2017 года, однако обе палаты Конгресса США (Сенат: 50-48; Палата представителей: 215-205) проголосовали против их принятия, посчитав, что Комиссия FCC превысила свою компетенцию их приятием и они «обременительны» для компаний интернет-провайдеров.

Это решение Конгресса США после его одобрения президентом США будет означать отмену Правил Privacy Rules. Соответственно, отмена Правил Privacy Rules, во-первых, фактически лишит Комиссию FCC права принимать аналогичные правила конфиденциальности для компаний интернет-провайдеров; во-вторых, усилит позиции таких компаний-гигантов широкополосного доступа к Интернету, как Comcast, Verizon, AT&T и др. (по отношению к компаниям Google, Facebook и др.), и в практическом плане даст им возможность не только осуществлять сбор данных, но и предоставлять их третьим лицам .

Формально-юридическая отмена Правил Privacy Rules не повлияет на действие «Правил сохранения открытости Интернета» (Rules to Protect Open Internet), принятых Комиссией FCC 26 февраля 2015 года, (далее – «Правила Open Internet») . Согласно Правилам Open Internet, требование защиты конфиденциальности пользователей является ключевым; функционирование широкополосной связи основано на трех основополагающих принципах: скорость, справедливость доступа и открытость Интернета; Комиссия FCC обладает полномочиями решать споры о соединении в каждом конкретном случае .

Интригу добавляет и то, что деятельность компаний Google, Facebook, Netflix и др., которые также осуществляют сбор данных пользователей, находится в компетенции Федеральной комиссии по торговле США (Federal Trade Commission, FTC) . Комиссия FCC и Федеральная комиссия по торговле США 1 марта 2017 года выступили с заявлением – «Совместное заявление исполняющей обязанности председателя FTC Морин К. Ольхаузен и председателя FCC Аджита Пайя о защите конфиденциальности в Интернете для американцев» (Joint Statement of Acting FTC Chairman Maureen K. Ohlhausenh and FCC Chairman Ajit Pai on Protecting Americans' Online Privacy) . Содержание документа не снимает существующей интриги и в общем плане подтверждает высказанное ранее утверждение о том, что в США на федеральном уровне нормативное регулирование в сфере сбора данных пользователей диверсифицируется .

Материал статьи подготовлен с использованием базы "Консультант".

Касенова Мадина – д.ю.н., профессор, заведующая кафедрой международного частного права Дипломатической академии МИД России, почетный профессор Дипломатической академии МИД России. Автор ряда исследований (монографии, научные статьи, сборники документов и материалов и др. общим объемом 235 п.л.) по вопросам международного частного права, международного права, трансграничного использования Интернета, международной информационной безопасности.

Член Международной ассоциации международного права (Лондон), член Российской ассоциации международного права (Москва). Эксперт кластера по информационной безопасности Ассоциации электронных коммуникаций (НП «РАЭК»), ведущий эксперт Института исследований Интернета (ИИИ), эксперт рабочей группы «Связь и информационные технологии» при правительстве РФ (2014 – настоящее время), ведущий эксперт Экспертного совета Института развития Интернета, ЭС ИРИ, эксперт комитета по вопросам управления Интернетом Автономной некоммерческой организации «Координационный центр национального домена сети Интернет».

Утечки данных. Рекомендации

Избранные главы «Отчета о глобальном Интернете 2016», Global Internet Report 2016

Утечки данных являются существенной проблемой по всему миру. Тем не менее, несмотря на растущее осознание рисков, они все равно происходят, подрывая доверие пользователей к Интернету. Стремясь понять проблему, авторы отчета анализируют экономические причины, которые могут противодействовать инвестированию в адекватные меры защиты данных и принятию таких мер. В отчете содержится пять рекомендаций по решению поднятых нами проблем касательно экономики утечек данных. Все эти меры подкрепляют друг друга, образуя своего рода кольцо безопасности данных.

Утечки данных являются существенной проблемой по всему миру. Тем не менее, несмотря на растущее осознание рисков, они все равно происходят, подрывая доверие пользователей к Интернету. Стремясь понять проблему, авторы отчета анализируют экономические причины, которые могут противодействовать инвестированию в адекватные меры защиты данных и принятию таких мер. В отчете содержится пять рекомендаций по решению поднятых нами проблем касательно экономики утечек данных. Все эти меры подкрепляют друг друга, образуя своего рода кольцо безопасности данных.

Первая рекомендация – поместить пользователей, являющихся конечными жертвами утечек, в центр решений по борьбе с утечками. Дополнительное ускорение этой мере придаст наша вторая рекомендация: больше открытости в обсуждении рисков утечки данных, инцидентов и их эффекта в мировом масштабе. Благодаря этому безопасность данных станет осознаваться как приоритетная задача, а значит, возникнет спрос на лучшие средства безопасности и методы профилактики/смягчения последствий.

Чтобы повысить экономические стимулы для внедрения этих средств в организациях, необходимо увеличить их ответственность, в том числе и финансовую, в случае утечки данных. В то же время организации, вложившие средства в лучшие меры защиты против утечек данных, должны иметь возможность убедительно сообщать об этом рынку, чтобы получить преимущество от вложений в безопасность. В основе этих пяти рекомендаций лежат два важных принципа: ответственность за данные (Data Stewardship) и коллективная ответственность.

Мы понимаем, что приведенные рекомендации являются средне- и долгосрочными, и что необходимо участие всех заинтересованных сторон. В качестве отправной точки мы приведем ряд советов по ключевым моментам того, как начать процесс внедрения наших рекомендаций. Мы хотим начать диалог и задать направление, а не навязывать собственные решения.

Принципы

В основе пяти рекомендаций лежат следующие высокоуровневые принципы:

Ответственность за данные (Data Stewardship)

Организации должны считать себя хранителями данных пользователей, защищая их данные не только потому, что того требует бизнес, но и от имени самих пользователей. Это соответствует приведенной ниже рекомендации об ориентации на пользователя. Пользователи хотели бы, чтобы организации обращались с их личными данными не только как с источником дохода. Организациям следует внедрить этичный подход к работе с данными и осознать, что делать добро выгодно: защита данных пользователей должна стать самоцелью, которая при этом защищает организацию.

Коллективная ответственность

Интернет один на всех. Одна утечка может привести к другой: «твоя проблема может стать моей проблемой». Организации несут общую ответственность с другими заинтересованными сторонами за обеспечение безопасности экосистемы данных в целом (см. http://www.internetsociety.org/collaborativesecurity). Например, поставщики могут предоставить решения, облегчающие профилактику утечек; сотрудники должны защищать свою работу от хакеров и случайного разглашения; госорганы могут внести свой вклад, формируя среду, способствующую появлению лучших решений для безопасности; другие стороны также могут играть важную роль, разрабатывая независимые стандарты и осуществляя обзоры для каждой области безопасности данных. Если хотя бы одна из этих связей не работает, под угрозой оказывается вся цепочка доверия.

Рекомендации

P1 ОРИЕНТАЦИЯ НА ПОЛЬЗОВАТЕЛЯ

Помещайте пользователей в центр решений, а при анализе потерь от утечек данных

учитывайте потери пользователей наравне с потерями организаций.

Internet Society давно уже борется за ориентированный на пользователя подход к проблемам Интернета (http://www.internetsociety.org/preserving-user-centric-internet). Такой подход ставит во главу угла пользователей и их потребности. В наших работах по этой тематике мы считаем пользователей тем элементом утечек данных, про само существование которого часто забывают, хотя в конечном счете именно пользователи оказываются главными жертвами.

В частности, при возникновении утечки данных:

- Пользователи могут даже не знать об утечке, так как многие организации не оповещают их, в том числе из-за отсутствия требований об уведомлении во многих странах.
- Даже если пользователи знают об утечке, их возможности чаще всего ограничены - раз утекшие данные уже не вернуть. Пользователям трудно бывает добиться финансовой компенсации за убытки, особенно если они не могут продемонстрировать прямой ущерб. Также пользователи могут столкнуться с повышенным риском кражи идентичности и другими видами ущерба. Кроме того, есть и нефинансовые аспекты, которые трудно компенсировать.
- Воздействие утечки на пользователей, как правило, изучается лишь в той степени, в которой это касается благосостояния организации, т.е. в плане компенсации прямого ущерба, кредитной защиты и удара по лояльности потребителей, но не с точки зрения ущерба для пользователей и общества в целом.

Эта ситуация должна измениться. Оценивая воздействие на пользователей, следует также учитывать затраты времени и средств на борьбу с мошенническими действиями, ставшими возможными в результате утечки; нефинансовый ущерб; будущие убытки. Большее внимание к полному воздействию утечек на пользователей поможет выработать более ориентированные на пользователей решения по борьбе с утечками. Если говорить более общо, то от каждой утечки расходятся «круги по воде», распространяя недоверие от пострадавших пользователей ко всем остальным. А чем меньше в Интернете доверия, тем меньше преимуществ для всех нас.

P2 ПРОЗРАЧНОСТЬ

Повышайте прозрачность, сообщая об утечках своевременно и подробно.

Мы выступаем за то, чтобы прилагать больше усилий к изучению постоянно меняющегося риска утечек данных, начиная с большей прозрачности информации об инцидентах, их причинах и последствиях по всему миру. Наша цель – создать таким образом спрос на решения, обрисованные в последующих рекомендациях. Требование оповещать об утечках данных увеличивает прозрачность – так мы можем определить, какие цели чаще атакуют, какие меры безопасности работают и какие нет, какие данные попадают к хакерам, как осуществляется сама утечка. Большая часть этой статьи основана на имеющейся информации о реальных утечках данных.

Ответственный обмен информацией дает организациям целый ряд преимуществ – он может помочь организациям упрочить свою защиту данных в глобальном масштабе, разработчикам политик – совершенствовать политики, регуляторам – преследовать злоумышленников, индустрии защиты данных – вырабатывать лучшие решения. Все это защищает экосистему данных в целом. Довести прозрачность до уровня действий – часть той ответственности, которую мы должны коллективно взять на себя, чтобы добиться, чтобы каждый мог принимать информированные решения, помогать в предотвращении утечек и снижать ущерб от тех, которые все-таки произошли. Если рынок не дает организациям стимула добровольно сообщать об утечках данных, что создает асимметрию информации, может потребоваться вмешательство государства.

P3 ПРИОРИТЕТ БЕЗОПАСНОСТИ

Безопасность данных должна стать приоритетной. Необходимо создать лучшие методы и инструменты для этой сферы. Организации должны следовать стандартам и передовой практике в области безопасности данных.

Как мы видели в разделе «Проблемы», уже имеется масса инструментов для профилактики утечек данных и минимизации их последствий. Однако организации, ответственные за работу с данными пользователей, используют эти инструменты не всегда. Почему же их использование не повсеместно, в свете потерь от утечек данных? Причина этого – частью в невежестве, частью в отсутствии экономических стимулов. Но не следует сбрасывать со счетов то обстоятельство, что даже при самых лучших намерениях работа с этими инструментами не всегда проста. Нам необходимо многое сделать для того, чтобы защита данных стала лучше применимой: облегчить или вовсе автоматизировать использование средств профилактики утечек или снижения тяжести их последствий. Ниже приведена «дорожная карта» инструментов и методов, которые мы рекомендуем в этом разделе.

Применимая безопасность (Usable Security)

В защите данных важную роль играет человеческий фактор. Например, пароль пользователя всегда является болевой точкой для безопасности. Достаточно ли он надежен? Регулярно ли меняется? Уникален ли? Знает ли его пользователь наизусть? Надежны ли требования к паролю? Защищен ли пароль от социального инжиниринга? По личному опыту можем сказать: как минимум на один из этих вопросов ответ, как правило, отрицательный. А этого уже бывает достаточно для утечки. Вот почему практики, инструменты и методы безопасности должны проектироваться с учетом человеческого фактора, чтобы они были применимы реально. Безопасность надо встраивать в инструменты работы с данными с самого начала, а не добавлять в последнюю очередь. Это и есть принцип безопасности на конструктивном уровне. И поскольку все мы люди, нас надо везде, где возможно, подталкивать к реализации средств безопасности.

Мы не намерены превращать эту статью в справочник по предотвращению утечек данных – для надежной профилактики требуется глубокий и многосторонний подход, описание которого выходит далеко за рамки нашего отчета. Безопасность данных – отдельная область деятельности, и внедрение архитектуры безопасности требует значительных ресурсов и обучения. А в нашем отчете мы всего лишь вычленим ряд усовершенствований, которые помогут предотвращать утечки данных независимо от архитектуры безопасности. Многие из этих принципов – такие как регулярное обновление ПО и задание паролей – хорошо понятны пользователям независимо от опыта и квалификации. Организации должны использовать эти меры и пропагандировать их среди сотрудников, но этого мало, если вспомнить о нашей коллективной от-

ветственности за безопасность Интернета: те же меры пользователи могут применять на личных устройствах и системах.

Мы подробно рассмотрим эти принципы, чтобы убедить организации более серьезно относиться к безопасности, в том числе предоставлять частным лицам инструменты для самозащиты от утечек не только как сотрудникам, но и как пользователям.

Пять основных рекомендаций

Профилактика утечек данных

Известные уязвимости

Как уже говорилось, многие утечки данных можно было бы предотвратить, если бы были закрыты известные уязвимости в системе. Поэтому, говоря о профилактике утечек, этот вопрос нельзя обойти вниманием. Всеобщая доступность Интернета не только делает его уязвимым для атак, но и дает доступ к средствам предотвращения утечек и других инцидентов, таким как программные патчи.

Например, для поддержания ПО в актуальном состоянии (в первую очередь это касается критических обновлений безопасности) сначала Microsoft, а потом и Apple позволили коммерческим и частным пользователям использовать автообновление системы или же просто сделали обновления автоматическими по умолчанию (см. https://blogs.msdn.microsoft.com/b8/2011/11/14/minimizing-restarts-after-automatic-updating-in-windows-update/ и http://www.cnet.com/news/apple-updates-macs-without-asking-but-its-to-foil-hackers/). Многие разработчики ПО также стали планировать выпуск обновлений на конкретное время, чтобы организации могли адаптировать собственные графики развертывания обновлений (Microsoft, например, публикует патчи во второй вторник каждого месяца). Здесь принцип «подталкивания» вроде бы неплохо работает, по крайней мере, на уровне отдельных устройств.

Однако на уровне корпоративных систем обновление ПО существенно сложнее: тут может потребоваться предварительное тестирование, составление внутреннего графика, разработка мер для старого оборудования, которое может уже не поддерживать обновленное ПО, а также действия по охвату личного оборудования сотрудников. Да и сам программный патч, закрывая старые уязвимости, может привнести новые либо иметь неожиданные последствия на разном оборудовании и программном обеспечении, которые придется учитывать.

В устранении известных уязвимостей нет волшебной палочки: существующие IT-системы нельзя заменить в одночасье, а новые системы привносят с собой новые проблемы. Так или иначе, распространение знаний о рисках утечек данных должно привести к реализации принципа безопасности на конструктивном уровне на всех этапах проектирования, как у разработчиков, так и у организаций, внедряющих их решения.

Социальный инжиниринг

Многие случаи утечки данных являются результатом социального инжиниринга, в частности, фишинга. Для борьбы с этой угрозой необходимо заниматься просвещением о рисках, а организации должны внедрить коллективную ответственность сотрудников за безопасность, одновременно предоставляя им нужные технологии и обучение. Сотрудников нужно учить тому, как не стать жертвой фишинговой атаки, в том числе, как распознать мошенническое письмо, почему нельзя щелкать по неизвестным вложениям, как и куда сообщить о подозрительной активности.

На более глубоком уровне сотрудники должны понимать риски, которые подобные атаки несут для организации. Можно начать с известных примеров, освещенных в печати: как сотрудник интернет-провайдера ненамеренно раскрыл электронный адрес директора ЦРУ (https://www.theguardian.com/technology/2016/sep/13/cia-john-brennan-hacking-trial), или какую роль социальный инжиниринг и стандартные пароли сыграли во взломе Target (http://krebsonsecurity.com/2014/05/the-target-breach-by-the-numbers/). Сотрудники должны понимать, что результаты утечки данных могут быть катастрофическими, включая информа-

цию о личной жизни пользователей (Ashley Madison, https://securityintelligence.com/two-important-lessons-from-the-ashley-madison-breach/), данные о сотрудниках (Управление кадровой службы США, https://arstechnica.com/security/2015/06/report-hack-of-government-employee-records-discovered-by-product-demo/32/), сведения о зарплатах и компрометирующие письма (Sony, https://en.wikipedia.org/wiki/Sony_Pictures_hack). Не говоря уже о том, что все это влияет на конечные результаты самой компании со связанными рисками для компенсации или дальнейшей занятости.

Технологии (такие, как почтовые спам-фильтры и веб-фильтры) помогают снизить риск мошеннических атак, открывающих дорогу к утечкам данных. Технологии также помогают защищать системы от атак с использованием информации, полученной в результате социального инжиниринга. Например, замена простого пароля на усложненные виды аутентификации (например, двухфакторную аутентификацию) может предотвратить несанкционированный доступ. Эти меры следует распространить и на сотрудников, использующих собственные смартфоны или компьютеры для работы. Аналогично, хотя и важно объяснить сотрудникам, почему нельзя втыкать в компьютер взявшиеся непонятно откуда устройства, которые могут переносить компьютерные инфекции, как, например, флэшки, лучше в дополнение к этому просто закрыть возможность автозапуска неизвестных устройств при подключении (https://www.schneier.com/blog/archives/2011/06/yet_another_peo.html).

Еще одна важная проблема – пароли. По нашему мнению, проблемной является безопасность как пользовательских паролей, так и паролей, хранящихся в организации. Мы придерживаемся того мнения, что инструменты аутентификации нуждаются в доработке, с тем, чтобы устранить вновь и вновь проявляющиеся пробелы в безопасности, вызванные как человеческим фактором, так и техническими дефектами. Кроме того, любые сохраненные пароли нужно надежно шифровать.

Одним из распространенных методов укрепления аутентификации является использование надежных, уникальных паролей, хранящихся в надежном менеджере паролей; другим – двухфакторная аутентификация. Оба метода широко известны, но, как показывает анализ примеров, не всегда используются. Ни один из них не дает 100% безопасности, и организациям и пользователям следует взвесить все «за» и «против» при выборе этих и других методов упрочения аутентификации и авторизации. Здесь мы говорим о них как о примерах проблем, возникающих при упрочении безопасности, а вовсе не как о самых лучших и уж тем более не единственных решениях для борьбы с социальным инжинирингом.

Смягчение последствий утечки данных

Хотя часть утечек данных можно предотвратить, но все-таки 100% безопасность и 100% свобода от рисков недостижимы. Систему можно взломать с помощью уязвимости нулевого дня; ошибка может привести к публикации данных; компьютер с данными может стать жертвой кражи или потери. Однако, во-первых, могут «утечь» лишь те данные, которые где-то хранятся, а во-вторых, если данные невозможно прочесть, их нельзя и использовать. Именно эти два метода смягчения последствий утечек – минимизацию данных и шифрование – мы сейчас и обсудим. Оба эти метода должны реализовываться в составе более широкой деловой и технической практики.

Минимизация данных

Нам попадались ситуации, где организации хранили лишние данные, значительно увеличившие цену утечки. Управление кадровой службы США хранило данные о бывших сотрудниках, а Ashley Madison – данные о пользователях, заплативших за удаление информации о себе. Здесь, разумеется, не все так просто. Понятно, что организация имеет четкий коммерческий мотив собирать данные, которые можно монетизировать (сейчас или потом), особенно в наше время, когда затраты на хранение данных стали просто копеечными. В некоторых случаях это может быть удобно и пользователю: например, если компания хранит информацию о кредитных картах для упрощения будущих покупок или оформления долгосрочной подписки.

С другой стороны, большой «улов» разнообразных данных имеет два крупных недостатка, а именно использование этих данных по назначению и нет. Даже при использовании данных по назначению встают вопросы конфиденциальности, поскольку наборы данных все растут в размере и могут комбинироваться с другими наборами, выдавая совершенно непредусмотренные результаты.

Кроме того, существует много случаев использования наших личных данных не по назначению, где минимизация данных может помочь минимизировать последствия. Кроме утечки данных, данные могут быть использованы спецслужбами для наблюдения за гражданами, или в преступных целях (подробнее о злоупотреблении данными см. https://www.bcgperspectives.com/content/articles/big-data-advanced-analyticstechnology-digital-bridging-trust-gap-hidden-landmine-big-data/?utm_source=201607&utm_medium=Email&utm_campaign=Ealert). Уже поэтому организациям стоит минимизировать объем собираемых данных, даже если они абсолютно защищены от взлома. Пользователям же следует насторожиться, если у них запрашивают больше данных, чем требуется, например, если приложение, включающее фонарик в мобильном телефоне, вдруг включает в лицензионное соглашение право доступа к данным местонахождения (http://www.techrepublic.com/blog/it-security/why-does-an-android-flashlight-app-need-gps-permission/).

Организациям следует четко и информированно оценить риск утечки данных, а затем по каждому элементу данных определить, превышает ли его ценность потенциальный дополнительный ущерб и убытки для пользователей в случае утечки. Например, в США номер социального страхования (SSN) – ключевой элемент информации при мошенничествах с выдачей себя за другое лицо. Если организации нужен идентификатор пользователя, то она должна задать себе следующие вопросы:

Обязательно ли использовать в качестве идентификатора SSN или другой идентификатор, присваиваемый государством?

Если да, то нужно ли хранить государственный идентификатор после установления идентичности пользователя, или же можно использовать/создать другой ИД?

Если необходимо использовать государственный идентификатор в качестве ИД, можно ли его отделить от остальной личной информации?

Такой анализ позволит определить, какие данные необходимо собирать и хранить, какое время должны храниться такие важные данные и когда они подлежат удалению. Также он должен принять по внимание ценность данных не только для организации, но и для сотрудника или заказчика, принимая во внимание не только преимущества от использования данных по назначению, но и вред от их попадания в чужие руки или

злоупотребления ими. Этот подход к данным входит в концепцию Data Stewardship. Разумеется, трудно преодолеть давление рынка, побуждающее собирать и накапливать все больше данных; поэтому принцип минимизации данных, возможно, потребуется включить в национальное законодательство о конфиденциальности данных и выработать рекомендации по внедрению важных практических методов.

Шифрование

Internet Society считает, что шифрование должно быть нормой для передачи и хранения данных в Интернете. Более конкретно, организации должны использовать такой уровень шифрования, чтобы затраты времени и денег на дешифровку (если она вообще возможна) перевешивали любые возможные преимущества для атакующего. Цена экономии на шифровании четко видна во многих проанализированных примерах: Target, Департамент кадровой службы США и другие вообще не шифровали данные, в то время как TalkTalk, Корейский центр фармацевтической информации (https://www.databreaches.net/43-million-south-koreans-had-their-medical-information-leaked/) и другие использовали слишком слабое шифрование. Более того, шифрование не является статичным – как видно из истории Ashley Madison, по мере появления более продвинутых систем шифрования, они должны применяться не только к новым учетным записям, но и к уже существующим (http://www.pcworld.com/article/2982919/security/ashley-madison-coding-blunder-made-over-11-millionpasswords-easy-to-crack.html).

Экономические причины отсутствующего или слабого шифрования двояки: стоимость правильной реализации надежного шифрования считается слишком высокой, а его преимущества недостаточно высокими. Однако сейчас ситуация начинает меняться.

В последние годы шифрование стало применяться гораздо шире: например, WhatsApp шифрует сообщения, а Apple – данные, хранящиеся в устройствах и в облаке. Частично это происходит в ответ на сообщения о прослушивании со стороны спецслужб, а частично - в ответ на риски безопасности данных. Независимо от мотивов, преимущества шифрования в плане снижения ущерба от утечек никуда не деваются.

Детальная информация о шифровании носит технический характер и безусловно выходит за рамки этого отчета. Наши принципы, однако же, ясны: безопасность должна быть реализована на конструктивном уровне и должна подталкивать пользователя к использованию достаточно надежного шифрования как можно более прозрачным образом (или реализовывать такое шифрование по умолчанию).

Шифрование должно быть спроектировано, учитывая нужды пользователя, а не наоборот. Оно должно быть доступным, дешевым и простым в применении - как для связи по Интернету, так и для работы с сайтами, для всех устройств и облачных сервисов.

Сейчас, когда все больше сотрудников работает из дома или в пути, или же в офисе на личном оборудовании, организации очень и очень заинтересованы в том, чтобы их сотрудники использовали надежные технологии шифрования. В свою очередь сотрудники должны понимать потенциальный риск пренебрежения шифрованием и для своего работодателя, и для клиентов, чтобы не стать слабым звеном в системе безопасности.

Экономические стимулы

Разумеется, сколь бы дружественными для пользователя ни были инструменты, они все равно стоят денег и времени на внедрение, и не каждая организация может себе это позволить. Рынок, регулирующий инвестиции в кибербезопасность, с экономической точки зрения несостоятелен. Во-первых, у утечек данных есть экстерналии, не учитываемые организациями, что снижает их мотивацию инвестировать в безопасность. Во-вторых, даже там, где такие инвестиции делаются, асимметрия информации затрудняет оповещение всей экосистемы о результирующем уровне кибербезопасности. Сейчас мы рассмотрим, как можно бороться с несостоятельностью рынка путем экономических стимулов, как затрат, так и преимуществ.

ПОВЫШЕНИЕ ОТВЕТСТВЕННОСТИ. Если возложить большую ответственность за экстерналии в результате утечки данных на организацию, хранившую эти данные, то цена утечки возрастет, что побудит организации усилить защиту от утечек и минимизировать их последствия. С экономической точки зрения, здесь целью является интернализация ущерба от утечки данных для организации-виновника.

СИГНАЛЫ О БЕЗОПАСНОСТИ. Если организации смогут сигнализировать, что они менее уязвимы, они обретут конкурентное преимущество, что даст стимул инвестировать в профилактику утечек. С экономической точки зрения, здесь целью является возможность для организаций убедительно сообщать о своем уровне кибербезопасности.

Принципы, укрепляющие экономические стимулы

Интернализация экстерналий увеличит цену утечки данных для организации и создаст дополнительный стимул избежать утечки. Однако здесь действуют и более широкие соображения безопасности и экономики, по отношению к которым все мы несем коллективную ответственность. Например, обучение сотрудников борьбе с социальным инжинирингом не только помогает избежать прямой утечки данных, но и помогает защититься от атак на другие организации, с которыми сотрудник может взаимодействовать. Здесь у работодателя нет ни прямой ответственности, ни прямых преимуществ. Такая коллективная ответственность является принципом, лежащим в основе всего Интернета, и о нем нельзя забывать в стремлении предотвратить ту или иную конкретную утечку данных. Это краеугольный камень для создания здорового кольца безопасности данных.

Хотя мы уверены, что добросовестная ответственность за данные, безусловно, в экономических интересах самой организации (если вспомнить о цене утечки), мы также убеждены, что у каждой организации есть социальная ответственность за то, чтобы Интернет стал безопаснее для всех. Например, для корпорации профилактика утечек данных должна стать неотъемлемой частью корпоративной политики, а более широкий спектр усилий по повышению безопасности Интернета – частью социальной ответственности организации. В конце концов, чем больше доверия в Интернете, тем больше его преимущества для всех.

P4 ОТВЕТСТВЕННОСТЬ

Организации должны отвечать за свои утечки. Необходимо выработать общие правила распределения ответственности и компенсаций за утечки данных.

Как видим, ущерб от утечки данных может распределяться по широкому кругу пострадавших сторон. В случае Target банки понесли гигантские убытки на перевыпуск скомпрометированных кредитных карт; в случае Ashley Madison ущерб понесли пользователи и их близкие; в случае Sony значительная часть ущерба легла на плечи сотрудников и

членов их семей; а в случае Департамента кадровой службы – были скомпрометированы данные не только нынешних, но и бывших и потенциальных сотрудников.

Экономический стимул для предотвращения таких экстерналий при этом очень мал, именно потому, что они экстерналии, т.е. ложатся на других. Если же заставить организацию отвечать за экстерналии, то стимул избежать их увеличится. Как мы ожидаем, просвещение и повышение потенциального ущерба заставят организации более ответственно относиться к безопасности данных, включив ее в управление данными в качестве ключевого элемента.

Однако попытки интернализации экономических экстерналий относительно утечек данных могут столкнуться с рядом проблем.

Начнем с того, что для того, чтобы стимулы были максимально действенными, необходимо лучше понять и представить полный объем финансовых и нефинансовых убытков от утечек данных. Необходимо явно прописать общие правила распределения ответственности и компенсаций и добиться того, чтобы все заинтересованные стороны поняли их и могли принять соответствующие меры. В некоторых случаях могут потребоваться минимальные стандарты работы с данными, а если они не будут приняты добровольно, придется закрепить их законодательно (например, прописать положения безопасности данных и минимизации данных в законе).

Все это не умозрительные, а практические проблемы, поскольку в утечке может участвовать третья сторона, например, подрядчик Target, через которого был осуществлен взлом. У организации может быть множество поставщиков оборудования и ПО, которые могут сыграть свою роль в утечке. Даже если и можно определить вину, ответственность, возможно, распределится иначе: вспомним финансовые учреждения, которым пришлось возмещать стоимость перевыпуска карт. Эти правила не обязательно должны быть высечены в камне, поскольку судебные иски могут перекидывать ответственность с одной стороны на другую способами, которые невозможно предусмотреть.

С учетом масштаба проблем в области широкого распределения ответственности и наших целей мы сейчас более подробно рассмотрим ответственность за ущерб от утечек для пользователей.

В общем и целом, именно пользователи находятся в центре нашей миссии по укреплению доступности и доверия в Интернете, а эти цели гораздо труднее осуществимы, поскольку пользователи страдают от утечек данных, но при этом не имеют возможности напрямую контролировать их защиту. Более того, пользователи часто являются конечными жертвами утечек данных, будь то кража идентичности, кредитных карт или медицинской информации, но при этом их часто не учитывают при анализе того, как предотвращать утечки и снижать их последствия.

Как мы уже говорили выше, на сегодняшний день конечные пользователи являются отсутствующим звеном системы. Конечным пользователям не всегда сообщают об утечках их данных; они не всегда могут соотнести ущерб для себя с той или иной утечкой; а возможно, они вынуждены были отказаться от своего права на компенсацию в будущем для того, чтобы пользоваться услугой. Более того, там, где нет прямых отношений «поставщик-заказчик», у конечного пользователя в случае утечки может быть очень мало возможностей вернуть деньги или воспользоваться услугами кредитного мониторинга. Да и судиться с организацией для пользователя может оказаться не по средствам.

Рассмотрим некоторые из этих проблем. Во-первых, еще раз повторимся: мы твердо стоим на том, что оповещение об утечках в общем случае необходимо. Это тот шаг, который помогает установить ответственность. Благодаря ему те люди, чьи данные были затронуты утечкой, узнают об этом и смогут обезопасить себя (и потребовать компенсации – об этом ниже). Дополнительным преимуществом здесь является ущерб репутации организации, в которой произошла утечка, что повышает мотивацию к их профилактике. Поэтому об утечках оповещают чаще всего в тех странах, где того требует закон, как мы видим на примере США.

Отметим, что и у обязательного оповещения об утечках есть свои пределы – организация может не знать, что ее взломали, или не понимать, о чем ей надо сообщить и кому. Также не всегда просто выбрать оптимальное время для оповещения. Требования к оповещению тоже непросты: слишком много оповещений – и пользователи почувствуют себя беспомощными, слишком мало – забытыми (см. https://iapp.org/news/a/130-days-1500-notifications-does-dutch-breach-rule-foreshadow-gdpr/). Кроме того, хотя в оповещениях можно указывать информацию, которая может предотвратить другие утечки того же характера, очень не хотелось бы сообщать то, что помогало бы хакерам – а это всегда риск, когда речь идет о незакрытых известных «дырках». По мере того как разные страны будут набирать опыт и вырабатывать правила оповещения, а к ним будут присоединяться все новые и новые страны, со временем должен установиться правильный баланс.

Во-вторых, поставщики интернет-услуг имеют тенденцию жестко ограничивать свою ответственность и права пользователя на компенсацию. Вот, например, цитата из условий пользования одним из менеджеров паролей (так и было выделено всеми прописными буквами, см. https://www.dashlane.com/terms):

> ПОЛНЫЙ ОБЪЕМ НАШЕЙ ОТВЕТСТВЕННОСТИ ПЕРЕД ВАМИ ПО ЛЮБЫМ ПРЕТЕНЗИЯМ, ВОЗНИКАЮЩИМ ВСЛЕДСТВИЕ ИСПОЛЬЗОВАНИЯ САЙТА ИЛИ УСЛУГ ЛИБО В СВЯЗИ С НИМИ, ОГРАНИЧЕН СОВОКУПНО СУММОЙ В СТО ДОЛЛАРОВ США (U.S. $100,00).

А ведь такой менеджер может хранить сотни паролей, утечка которых способна вылиться для пользователей в сумму гораздо больше сотни долларов – перед нами яркий пример того, как компания перекладывает экстерналии на своих пользователей. Попадаются также и ограничения на право участия в коллективном иске (иске, объединяющем пользователей, оказавшихся в одной и той же ситуации), допускающие только индивидуальное разбирательство. Иными словами, если пользователь захочет вернуть хотя бы часть ущерба, ему предстоит долгая, трудная и потенциально дорогостоящая тяжба.

Простого ответа здесь нет: поставщики интернет-услуг вправе предлагать такие условия (в рамках законодательства о защите прав потребителей), а пользователи, разумеется, вправе отказываться от их услуг, если они прочли условия соглашения и сочли их неприемлемыми. Ситуацию могут исправить рыночные силы, которые увеличат спрос на более дружественные и справедливые условия, такие как повышенный порог ответственности (вследствие просвещения), либо законы, лишающие юридической

силы отказ от прав пользователей, таких как право на коллективный иск.

В случае розничной сети, такой как Target, клиенты вообще не пользовались интернет-услугами. Они расплачивались карточками в магазине, и лишь в момент оплаты их данные были доступны для утечки. Коллективный иск покупателей к Target закончился мировым соглашением, но часто подобные иски отклоняются судом за отсутствием доказуемого финансового ущерба. Получается, что у пользователей нет прав на собственные данные, если только они не могут продемонстрировать прямой количественно оцениваемый ущерб, а ведь, по идее, они должны обладать естественным правом на защиту от утечек данных.

Не всегда ясно, какими правами обладают пользователи в случае утечки данных, и сейчас положение складывается отнюдь не в их пользу. Тем не менее, ряд стран уже сейчас укрепляет и разъясняет в своем законодательстве объем прав физических лиц в случае утечки данных. В конце концов, от пользователя может потребоваться доказать прямой ущерб для получения компенсации. Тут не учитывается ни долгосрочный риск стать жертвой мошенничества, ни затраты времени и денег на его предотвращение. Кроме того, компенсация может не покрывать нефинансовый ущерб.

В этой ситуации едва ли не все противоречит разумному ожиданию того, что права и интересы пользователей будут защищены в случае нарушения конфиденциальности их данных. Кроме фактического ущерба, как финансового, так и выраженного в потраченном времени, повышенный риск стать жертвой мошенничества в будущем должны тоже покрывать организации, допустившие утечку данных, а не жертвы, как сейчас.

СИГНАЛЫ О БЕЗОПАСНОСТИ

P5 Повышайте стимулы инвестировать в безопасность, оживляя рынок надежной, независимой оценки мер безопасности данных.

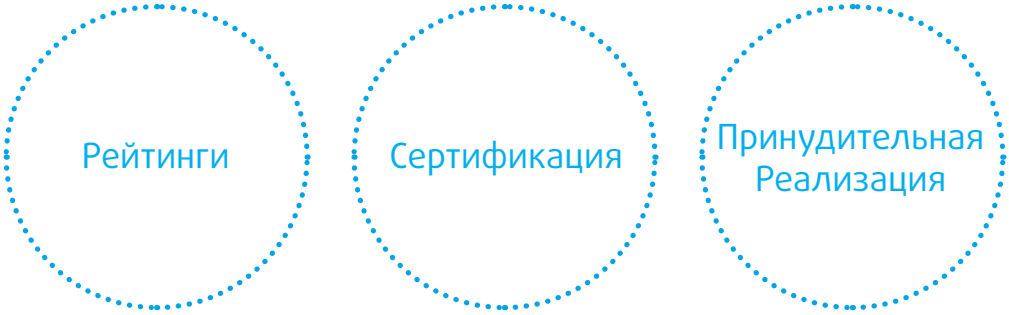
Все мы – заказчики, пользователи, сотрудники и даже организации, доверяя наши данные другой стороне, оказываемся в ситуации фундаментальной информационной асимметрии. От нее же страдают и сборщики данных, желающие получить преимущество от повышения собственной безопасности. В разделе «Проблемы» мы рассматривали ситуацию с рынком подержанных машин, где продавцу трудно продемонстрировать покупателю качество машины, и последующее вырождение авторынка в «рынок лимонов», так как плохие машины фактически вытесняют хорошие с рынка. Также мы видели, что даже у новых автомобилей имеется набор интересующих нас атрибутов и ряд способов проверить их наличие.

Как это применимо к нашей ситуации? Вернемся к примеру с менеджером паролей. Пользователи могут проверять поисковые атрибуты – например, облачная это услуга или нет, и составлять себе мнение об опытных атрибутах в рамках пробного пользования. Но оценить безопасность услуги заранее они не могут. К сожалению, тут до утечки ничего не узнать, а после утечки что-то делать уже поздно.

Вспомним также историю с Target и поговорим о подборе подрядчиков. И Target, и другие компании явно выбирали подрядчиков на основе критериев, связанных с предлагаемыми услугами – поставщика холодильного оборудования проверяли только на это. В той мере, в которой безопасность данных вообще играет роль до момента, когда поставщик получает право подключиться к информационной системе, очень трудно оценить безопасность систем и бизнес-практики каждого подрядчика без больших затрат. Как мы видим, у многих компаний проблемы с обеспечением безопасности собственных систем, не говоря уже об оценке безопасности каждого подрядчика, с чьими информационными системами приходится взаимодействовать.

Поэтому у организаций должна быть возможность сигнализировать пользователям, подрядчикам и сотрудникам о своем уровне защиты от утечек данных, а также других аспектах безопасности, включая безопасность устройств Интернета вещей. Как мы уже говорили, реализовать такие сигналы можно тремя способами: это рейтинги, сертификация и принудительная реализация.

Три главных способа подачи убедительного сигнала



Рейтинги. Журнал Consumer Reports уже начал составлять рейтинги программных продуктов по набору атрибутов, призванных помочь пользователю выбрать лучший программный продукт для защиты своих устройств. При всей полезности таких рейтингов они не затрагивают безопасность данных напрямую. Насколько нам известно, еще никто не начал осуществлять подобную оценку онлайн-услуг для потребителей. Она была бы полезна при принятии решений о том, какому интернет-банку, медицинскому сервису и т.п. доверить свою личную информацию. В то же время такая услуга могла бы давать полезную информацию, оценивая условия пользовательских соглашений с точки зрения безопасности данных и помогая пользователям выбрать лучшую защиту в случае утечки или ее попытки. Мы надеемся, что это подвигнет поставщиков онлайн-услуг к конкуренции за более дружественные к пользователю условия обслуживания в плане безопасности данных.

Еще один пример рейтингов в области безопасности: новая независимая компания начала составлять рейтинги безопасности организаций, что помогает страховым компаниям выбирать полисы киберстрахования. Эта компания, стартап под названием UpGuard, разработала рейтинг оценки угроз кибербезопасности (Cybersecurity Threat Assessment Rating, CSTAR), в котором уровень киберриска основывается на внешней оценке из общедоступных интернет-источников и внутреннего поиска (http://www.forbes.com/sites/brucerogers/2016/02/11/upguard-out-to-disrupt-7-5-billion-global-cybersecurity-insurancemarket/#6b7370112dda).

Сертификация. Некоторые подвижки в направлении создания процедуры сертификации безопасности данных уже имеются. UL, уже проводящая сертификацию широкого спектра электронных устройств, теперь сертифицирует и аспекты финансовой кибербезопасности, например, для кассовых терминалов, и начала разрабатывать стандарт сертификации устройств интернета вещей (http://www.ul.com/newsroom/pressreleases/ul-launches-cybersecurity-assurance-program/). А Пейтер Затко, известный специалист в области кибербезопасности, основал Независимую лабораторию кибертестирования (Cyber Independent Testing Laboratory) для сертификации безопасности устройств, ПО и услуг. По его замыслу, результаты тестирования должны быть похожи на информацию о пищевой ценности на упаковках продуктов, т.е. не просто сообщать о сертификации, но и содержать данные о разных атрибутах безопасности (также http://blogs.cfr.org/cyber/2015/12/18/qa-with-peiter-zatko-aka-mudge-setting-up-the-cyber-independenttesting-laboratory/). Кроме того, система правил международной безопасности APEC требует от сертификационных учреждений (агентов ответственности) сертифицировать уровень безопасности организации согласно требованиям программы (см. документ APEC Cross-Border Privacy Rules Program Requirements, который можно загрузить по адресу: http://www.cbprs.org/GeneralPages/APECCBPRSystemDocuments.aspx).

Процессы сертификации, главным образом, предназначены для того, чтобы помочь заказчикам (и организациям, и конечным пользователям) выбрать лучшие сервисы, что будет очень полезно. Также они повышают уровень прозрачности в индустрии.

Еще один подход заключается в том, чтобы поощрять внедрение признанных индустрией стандартов и передовой практики. Этот процесс может быть как сертифицируемым, так и самосертифицируемым. Например, Национальный институт стандартов и технологий США (NIST), работая совместно с заинтересованными сторонами, разработал систему кибербезопасности на основе президентского указа от 2013 года (https://www.nist.gov/cyberframework). Такие стандарты отражают передовую практику индустрии и являются добровольными, а не обязательными. Их внедрение помогает повысить безопасность организаций. Хотя соответствие нормам оценивается самой организацией, оно может использоваться как сигнал между партнерами, что они соответствуют определенным стандартам, перед вступлением в деловые отношения. Полное соответствие на сегодняшний момент ограничено, но этот подход довольно многообещающий.

Принудительная реализация. И, наконец, там, где независимых рейтингов или сертификации недостаточно или адекватные добровольные стандарты не приняты повсеместно, может потребоваться госрегулирование. Это особенно важно там, где несостоятельность рынка имеет значительные последствия – будь то большие суммы экстерналий или крайняя асимметрия информации. Минимальные требования к безопасности данных обычно содержатся в законах о конфиденциальности и защите данных. Как уже говорилось, есть ряд ситуаций, когда именно госрегулирование лучше всего подходит для борьбы с несостоятельностью рынка. В этом случае нашим принципом было бы регулирование результатов мер безопасности данных (например, чтобы сохраненные данные не могли быть прочитаны посторонними), а не инструменты или методы для ее обеспечения (такие, как тип шифрования), чтобы организации могли изобретать все более эффективные способы достижения нужного результата.

И, наконец, Internet Society верит в то, что свобода инновации (permissionless innovation) была и является главной движущей силой Интернета, где каждый может создать новую услугу или приложение, не получая на это предварительного разрешения ни от кого. Важно, чтобы никакие меры госрегулирования или сертификации не вступали в конфликт с этим принципом. Они должны применяться лишь в крайнем случае и быть спроектированы так, чтобы не представлять барьера для выхода на рынок (см. https://www.internetsociety.org/internet-invariants-what-really-matters).

Утечки данных являются все более острой проблемой во всем мире. Чтобы снизить остроту и экономический ущерб от этой проблемы, мы предлагаем изменить подход к борьбе с утечками, включив в нее все заинтересованные стороны. Так как пользователи переносят все большую часть собственной жизни в Интернет, раскрытие полного спектра его преимуществ по всему миру немыслимо без доверия пользователей. Это доверие зависит от того, насколько защищены данные пользователей от утечки. Каждая утечка создает новую группу обманутых пользователей, чей негативные опыт распространяется и на знакомых по принципу сарафанного радио, и через новостные отчеты, сея опасения, подрывая доверие пользователей в целом.

Хотя в конечном счете именно пользователи являются жертвами утечек данных, и именно их доверие страдает больше всего, сейчас ни пользователи, ни их доверие не находятся в фокусе мер по борьбе с утечками данных. Например, организации собирают и хранят больше пользовательских данных, чем нужно, и охраняют их хуже, чем могли бы. А после утечки оказывается, что у пользователей не так уж и много прав на защиту. Анализ потерь от утечек данных, в основном, учитывает ущерб организаций, а пользователи там «учитываются», в основном, в виде упущенной выгоды.

Internet Society предлагает переориентировать методологию борьбы с утечками данных так, чтобы пользователи оказались в ее центре, а организации приняли ответственность за вверенные им пользовательские данные, равно как и коллективную ответственность за повышение безопасности Интернета. Организациям также следует стать прозрачнее относительно происходящих утечек данных и их последствий. Благодаря этому безопасность данных станет приоритетной задачей, а значит, возникнет спрос на лучшие средства безопасности и методы профилактики/смягчения последствий. Чтобы у организаций был стимул использовать эти инструменты, нужно повысить их ответственность за убытки от утечек данных по сравнению с нынешним положением дел. Также они должны нести и больше расходов. Но в то же время у организаций должен появиться способ убедительно демонстрировать рынку наличие дополнительных мер предотвращения утечек данных.

Итоги

Очень показательна параллель между нынешней ситуацией в индустрии безопасности данных и попытками повысить безопасность автомобилей за последние 50 лет. Как ни трудно сегодня в это поверить, у ранних автомобилей не было ремней безопасности, детские автокресла появились только в 60-е годы прошлого века, а закон об обязательной установке подушек безопасности вызвал бурное сопротивление автопроизводителей.

Попытка Ford получить конкурентное преимущество, повысив безопасность автомобилей, была воспринята в США как провальный ход. Эти ранние средства обеспечивали пассивную безопасность, защищая пассажиров в случае аварии – в нашей тер-

минологии это средства смягчения последствий. Сегодня все они стали стандартными, и автопром наперебой вкладывает в безопасность большие деньги, разрабатывая все новые средства активной безопасности, призванные предотвращать столкновения, такие как автоматические тормоза. В нашей терминологии это средства профилактики.

За это время на рынке появилось множество хорошо узнаваемых движущих сил. Первым шло просвещение – независимые стороны, такие как Ральф Нейдер с его книгой 1965 года «Опасен на любой скорости» (Unsafe at any Speed), трубили во все трубы о нежелании индустрии внедрять меры безопасности. Затем появились обязательные государственные стандарты, вызвавшие сопротивление индустрии, такие как подушки безопасности; независимые организации занялись составлением рейтингов автомобилей; а госорганы принялись тестировать машины на безопасность при опасности столкновения с препятствием, включая знаменитый шведский «лосиный тест». Все это привело к значительному сокращению смертности при авариях (в пересчете на суммарный пробег). Говоря о будущем, многие полагают, что новые, полностью или частично автоматические машины, еще больше увеличат безопасность, автоматически избегая ДТП. И тут мы, пройдя полный круг, возвращаемся к теме нашего отчета.

Ведь автоматические автомобили будут управляться компьютером и иметь встроенные средства коммуникации с водителем, а возможно, и с другими машинами. В результате компьютер станет потенциальной жертвой дистанционного взлома, как уже случилось с Chrysler Jeep. Это может привести к значительной утечке данных о расположении и действиях водителей, не говоря уже о возможности перехвата управления автомобилем (а то и группой автомобилей).

В более широком плане многие из наших рекомендаций пригодны и для профилактики и предотвращения последствий утечек данных во всем спектре устройств интернета вещей. Мы говорим не только о данных, которые такие устройства собирают с помощью сенсоров, но и о пробелах в защите, могущих привести к рискам для личной или общественной безопасности, ярким примером которых являются автоуправляемые машины. Поэтому мы призываем применять выводы из этого отчета к соответствующим проблемам в сфере интернета вещей.

Источник: Global Internet Report 2016, https://www.internetsociety.org/globalinternetreport/2016/

Календарь событий: 2017 год

Международные события

29 мая - 2 июня
TNC17,
Линц, Австрия

Сетевая конференция TNC17 - это крупнейшая и самая престижная европейская конференция по исследованиям в области сетевых технологий. Более 650 участников принимают участие в этом ежегодном мероприятии. TNC объединяет руководителей, менеджеров, специалистов по сетевым технологиям, а также экспертов по управлению идентификацией и доступом из всех крупных европейских сетевых и исследовательских организаций, университетов, всемирных учреждений-партнеров, а также представителей промышленности. https://tnc17.geant.org/

5-7 июня
NANOG 70,
Белвью, США

Североамериканская горуппа сетевых операторов (The North American Network Operators Group, NANOG) является одной из самых активных профессиональных ассоциаций в области сетевой архитектуры, конфигурации и технического администрирования сетей в Интернете. Основной фокус NANOG – на технологиях и системах, обеспечивающих работу Интернета: система глобальной маршрутизации, DNS, пиринг и связность. NANOG имеет активный список рассылки и проводит конференции три раза в год. http://nanog.org/meetings/NANOG70/home

13-15 июня
M3AAWG 40th
General Meeting,
Лиссабон, Португалия

Встречи M3AAWG, которые открыты только для членов организации, являются мероприятиями с несколькими треками, которые проводятся три раза в год и в которых принимают участие более 300 участников. Ведущие отраслевые эксперты, исследователи и представители государственной политики обсуждают такие темы, как методы борьбы с ботнетами, вредоносное использование социальных сетей, мобильные злоупотребления и связанное с этими проблемами законодательство.
https://www.m3aawg.org/upcoming-meetings

26-29 июня
ICANN 59,
Йоханнесбург, ЮАР

Встречи ICANN проводятся три раза в год в различных регионах земного шара для того, чтобы предоставить возможность активным членам сообщества ICANN лично поучаствовать в обсуждении насущных проблем. Общей темой, конечно, является DNS - глобальная система трансляции имен. Здесь обсуждаются как технические вопросы обслуживания услуг DNS, так и юридические и бизнес-аспекты предоставления регистрационных услуг. https://meetings.icann.org/en/johannesburg59

16-21 июля
IETF 99,
Прага, Чехия

IETF (Internet Engineering Task Force) является одной из основных организаций по разработке стандартов в области Интернета. В основном работа в IETF проходит в многочисленных списках рассылки, соответствующих различным рабочим группам (этих групп более 100). Три раза в год IETF проводит недельные совещания, на которые приезжают разработчики протоколов, инженеры и операторы со всего мира (в среднем около 1200 участников из более 50 стран мира).
https://www.ietf.org/meeting/upcoming.html

22-26 октября
RIPE 75,
Дубай, ОАЭ

Встречи RIPE проводятся два раза в год и собирают более 500 участников для обсуждения вопросов политики распределения номерных ресурсов (IP-адресов и номеров автономных систем) в зоне обслуживания RIPE NCC, сотрудничества, а также технических вопросов, связанных с маршрутизацией, DNS, связностью, измерениями и инструментарием. Встреча длится 5 дней и начинается с двухдневной пленарной программы, за которой следуют несколько параллельных сессий заседаний рабочих групп. https://ripe75.ripe.net/

В России

23-24 мая, Санкт-Петербург

ENOG 13 / RIPE NCC

Региональный форум, где интернет-специалисты, занимающиеся важнейшими аспектами работы Интернета, обмениваются знаниями и опытом по темам, актуальным для России, СНГ и Восточной Европы. https://www.enog.org/enog-13/

24-26 мая, Сочи

КРОС-2017

Конференция российских операторов связи, ежегодно проводимая компанией "НАГ" для специалистов и руководителей телекоммуникационной отрасли. К участию допускаются исключительно действующие операторы связи. Системные интеграторы, производители оборудования и поставщики услуг допускаются к участию только после утверждения оргкомитетом. http://cros.nag.ru/

24-26 мая, Казань

IT&Security Forum

Одно из крупнейших событий IT-отрасли, освещающее широкий круг вопросов в области информатизации и защиты информации, а также использования современных технологий с целью повышения эффективности и конкурентоспособности бизнеса. http://www.itsecurityforum.ru/

24-26 мая, Иннополис

ЦИПР-2017

Актуальная межотраслевая площадка для глобального диалога представителей промышленности, профессионалов отрасли информационных технологий, телекома, оборонного комплекса, венчурных инвесторов и государства по вопросам развития цифровой экономики, несырьевого экспорта и обеспечения кибербезопасности. http://cipr.ru/

1 июня, Краснодар

Код информационной безопасности

Серия конференций, проходящая через 26 крупных городов России, Казахстана, Белоруссии, Грузии и Азербайджана. Информация о новинках и трендах в современных IT-угрозах и достижений в борьбе с ними. http://codeib.ru

В Москве

5-6 июня, Сколково

Frontend Conf 2017

Профессиональная конференция фронтенд-разработчиков: адаптивный дизайн и юзабилити, вёрстка, CSS и HTML, разработка на JavaScript, новые и популярные фреймворки, одностраничные приложения, архитектура, автоматизация и многое другое. http://frontendconf.ru/

5-6 июня, Сколково

Web-scale IT Conference 2017

Применение веб-технологий в разработке крупных и государственных проектов. Облачные архитектуры, микросервисы, agile-методология, сервисно-ориентированный подход и другие аспекты веб-культуры в enterprise. http://webscaleconf.ru/2017

17 июня, Москва

DevConf 2017

Конференция, посвященная ведущим технологиям программирования и веб-разработки. Нацелена на профессиональных веб-разработчиков и тех, кто мечтает ими стать. Она объединяет ВСЕ самые распространенные языки, при этом каждому выделен свой поток (зал). https://devconf.ru/ru

20 июня, Москва

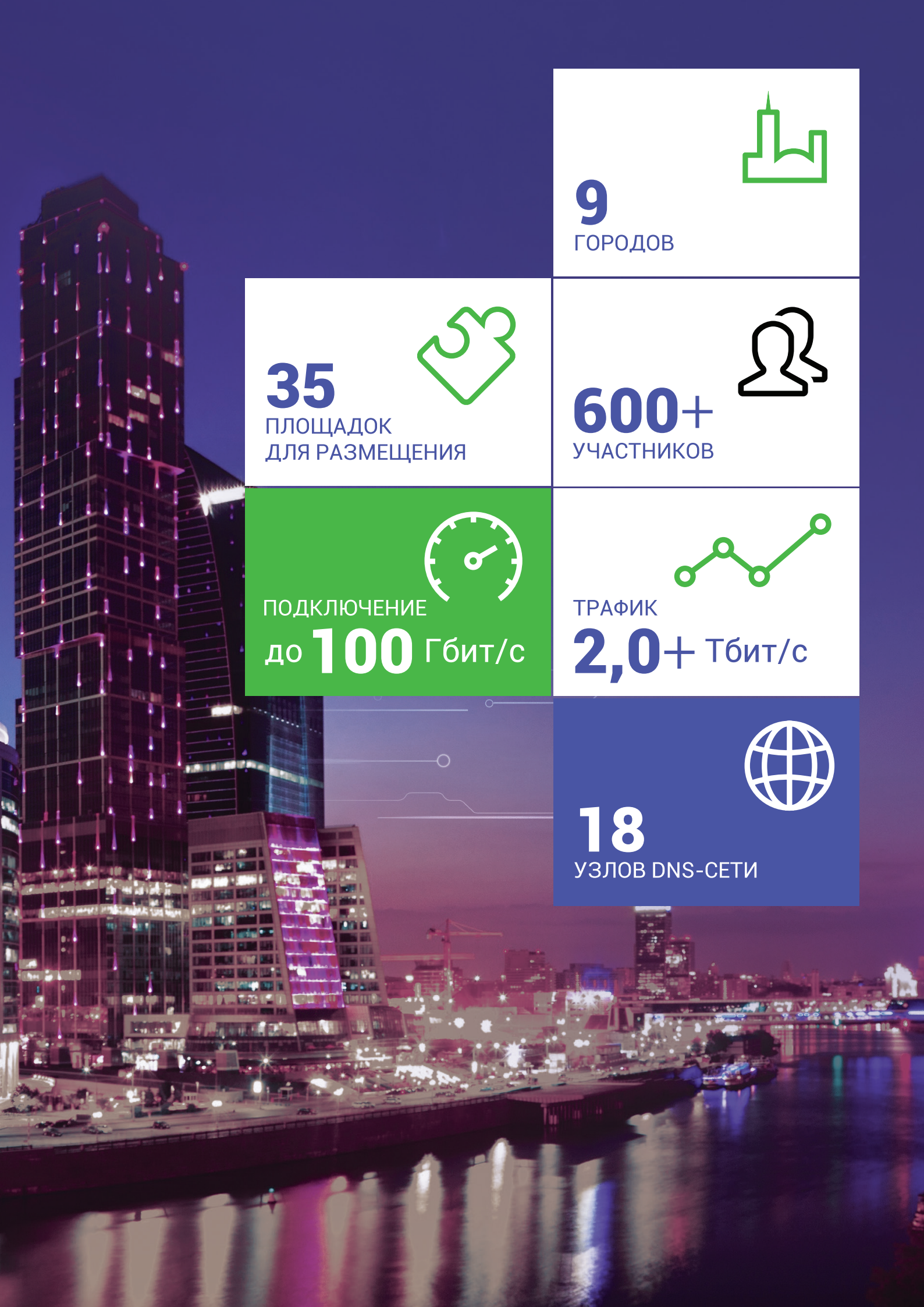
Future of Telecom 2017

Международный форум «Будущее телеком-индустрии» ставит своей целью продвижение инновационных технологий и установление профессионального сотрудничества между производителями аппаратных средств и разработчиками программного оборудования, представителями госорганов, руководителями отраслевых ассоциаций, менеджерами, аналитиками, экспертами и другими участниками мирового сообщества. http://www.telco-forum.ru/

MSK IX

WWW.MSK-IX.RU

+7 (495) 737-9295



9
ГОРОДОВ

35
ПЛОЩАДОК
ДЛЯ РАЗМЕЩЕНИЯ

600+
УЧАСТНИКОВ

ПОДКЛЮЧЕНИЕ
до **100** Гбит/с

ТРАФИК
2,0+ Тбит/с

18
УЗЛОВ DNS-СЕТИ

Интернет изнутри

2017